

UpdateEXPERT® Premium v7.01 Evaluation Guide



Information in this document is subject to change without notice. This document may be distributed freely only in whole, however no alterations are allowed without the expressed written consent of the author, St. Bernard Software, Inc.

© 2001-2005 St. Bernard Software, Inc. All rights reserved.

UpdateEXPERT is a registered trademark of St. Bernard Software, Inc. St. Bernard Software and the St. Bernard Software logo are trademarks of St. Bernard Software, Inc.

Microsoft, Windows, Windows NT, Windows 2000, .NET and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the USA and other countries.

All other product and corporate names may be trademarks or registered trademarks, and are used only for identification, without intent to infringe.

During installation you must agree with the end-user license agreement (EULA) before using UpdateEXPERT.

For more information about St. Bernard Software and UpdateEXPERT, check us out on the Web at <http://www.stbernard.com> and <http://www.updateexpert.com>.

Note: If you need assistance evaluating UpdateEXPERT, please contact our Technical Support department.

Contact Information

St. Bernard Software (North America, South America, Pacific Rim)

15015 Avenue of Science
San Diego, CA, 92128
Sales Phone: 800.782.3762
Sales Fax: 858-676-2299
Sales Email: sales@stbernard.com
Technical Support Phone: 858.676.5050
Technical Support Fax: 858.676.5055
Technical Support Email: support@stbernard.com

St. Bernard Software (Europe, Asia, Africa)

Unit 4
Riverside Way
Watchmoor Park, Camberley
Surrey, UK
GU15 3YQ
44.1276.401.640
Sales: 44.1276.401.640
Technical Support: 44.1276.401.642
Fax: 44.1276.684.479
Technical Support Email: support@uk.stbernard.com

Table of Contents

Note: TOC items are hyperlinks, use Mouse-Rollover, then click. Also, any reference to UpdateEXPERT in this manual implies UpdateEXPERT Premium.

Table of Contents.....	1
Purpose.....	3
UpdateEXPERT Premium Overview	3
Install UpdateEXPERT Premium.....	4
Identify the Web Proxy (if applicable)	10
Download the Latest UpdateEXPERT Database.....	11
Enumerate (Discover) Machines	11
Query your UpdateEXPERT Machine.....	12
Agentless Query Requirements.....	13
Download Patches	14
Named Policies (“Install Required” command).....	16
Conformance Reporting	17
Other Reports.....	18
Installing Master or Leaf-Agents.....	19
Leaf-Agent Configuration	21
What’s Next?.....	22
Validating Patches	23
Logging	24

SecurityEXPERT Overview	25
Configure SecurityEXPERT Web Proxy	26
Download SecurityEXPERT Templates.....	27
Creating a SecurityEXPERT Policy	28
Assigning the SecurityEXPERT Policy	31
Testing SecurityEXPERT Compliance.....	31
Modifying the SecurityEXPERT Policy.....	33
Enforcing the SecurityEXPERT Policy.....	33
Using Profiles with SecurityEXPERT	35
Thank You!.....	37
Appendix A – Custom Install Options	38

Purpose

The Evaluation Guide exists to assist in the *initial installation*, *basic usage*, and evaluation of UpdateEXPERT Premium. This is specifically intended to help evaluators make an informed decision towards the acquisition of a suitable patch and security settings management product.

UpdateEXPERT Premium Overview

Easy Installation – A “Typical” UpdateEXPERT Premium installation now includes settings management (SecurityEXPERT) in addition to patch management. MSDE is included (or you may use SQL Server if available) for storing Network-Tree data (such as machines & query results) and settings management data (security points & machine scans etc.). You may Install on any version of Win2K, XP Pro, and Win2003. IIS is required for Settings Management.

Unified Master-Agents – New for UpdateEXPERT Premium is support for simultaneous Master-Agent connections, easing administration in enterprise networks. See [“What’s New in UpdateEXPERT Premium”](#) for a menu of new UpdateEXPERT Premium features.

Agentless Patch Deployment – this allows patch deployment without installing Agents on client machines. Agentless deployment is appropriate for rapid patch deployment with minimal installation overhead. Agentless lets you meet urgent security policy requirements quickly.

Optional Agents - Leaf-Agents are not required, but are recommended for specific conditions or needs such as:

- Hardened Environments
- Disconnected* and/or *Wake-on-Lan* Machine Support
- Low-Bandwidth Connections
- Scaling (reduced network bandwidth use)

Leaf-Agents and additional Master-Agent deployments can be combined to support large or delegated patch management needs. The Administrator can deploy Agents to meet network needs, without incurring additional deployment costs.

Deployable Console - You can delegate patch management by deploying the console component to others. User “Roles & Rights” support granular access to capabilities.

Comprehensive Patch Database - SBS provides its own high-quality, independent and proprietary database for detection of installed vs. not-installed patches, and intelligent presentation of applicable patches for client machines. The Patch Install Wizard integrates with the database for grouping patches, presenting patch options, displaying diagnostic patch deployment messages, and controlling reboots. See the latest information on supported [OSes, Applications and Languages](#) (2 page PDF).

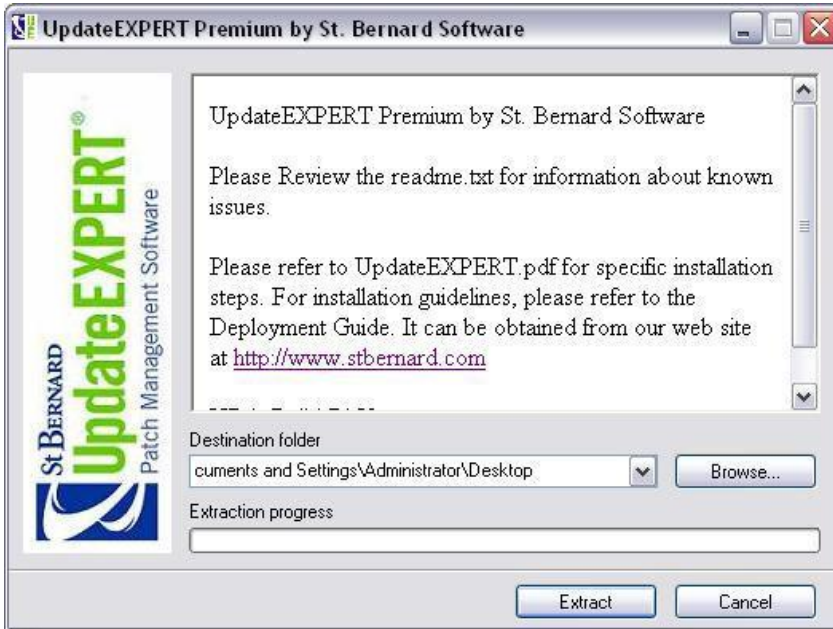
Private & Custom Fixes – Company specific (private) hotfixes from Microsoft can be added to the database upon request, then deployed company wide for your convenience. Non-supported or in-house patches may be deployable with Custom-Fix.

Installer Service - SBS provides its own installer/scheduling service (rather than Microsoft’s) that is persistent across reboots and shutdowns, ensuring patch installation occurs.

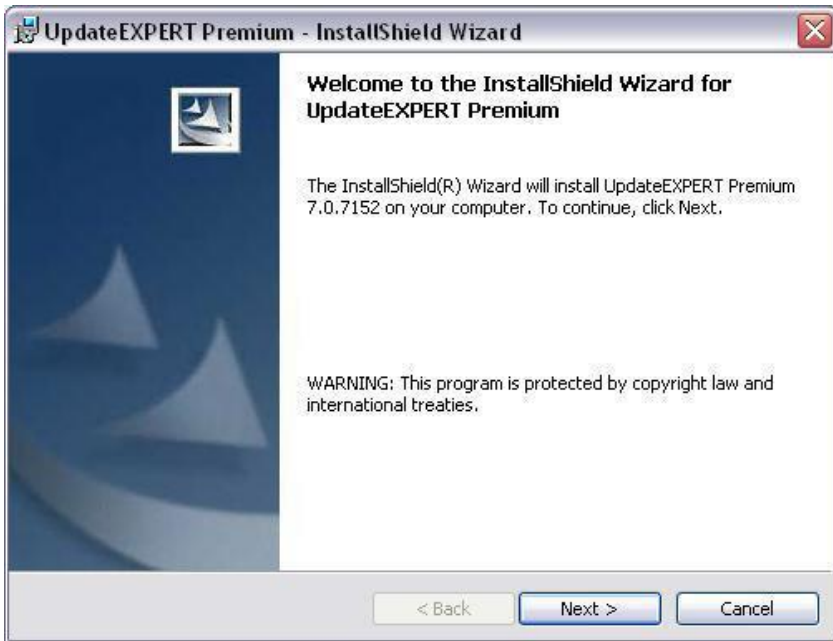
Disconnected Networks – SBS provides its own utility (upon request, at no charge) for updating UpdateEXPERT instances installed in non-internet connected networks.

Install UpdateEXPERT Premium

This Eval Guide example illustrates a new installation of UpdateEXPERT Premium. Login with Administrator privileges. [Download the UpdateEXPERT Trial Software](#). When prompted, click SAVE to download the compressed file (~120MB) to your local disk. When prompted again click RUN to launch the self-extraction dialogue (screen shot). In the example below a new folder with installation files in it will be created on the desktop for easy access to **Setup.exe**.



Double-click on **Setup.exe**. Click **Next**.



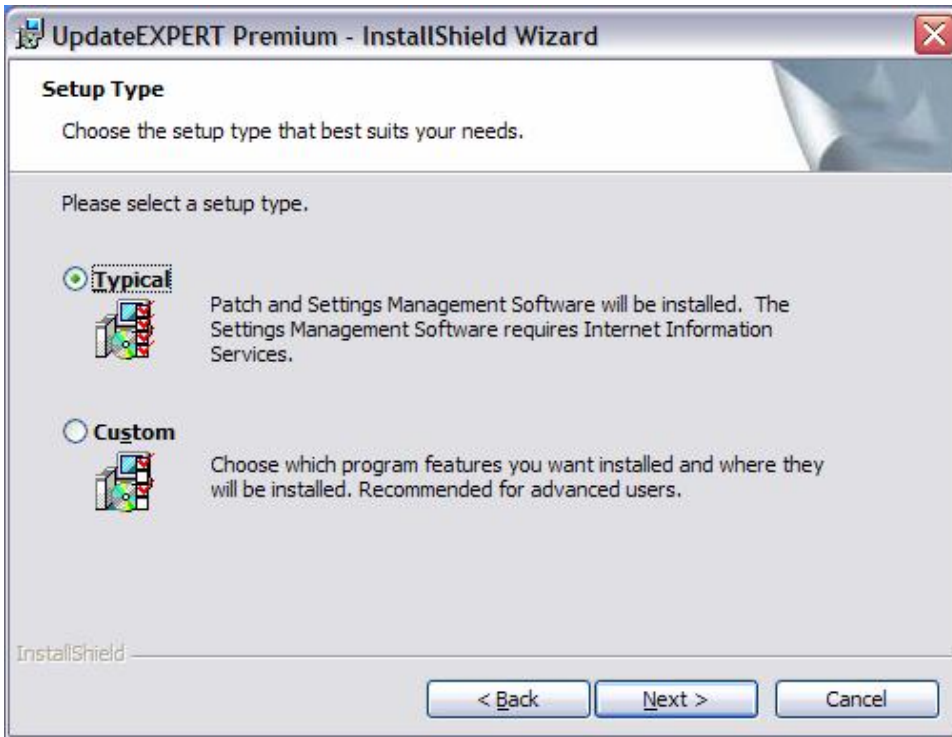
Click **Next**



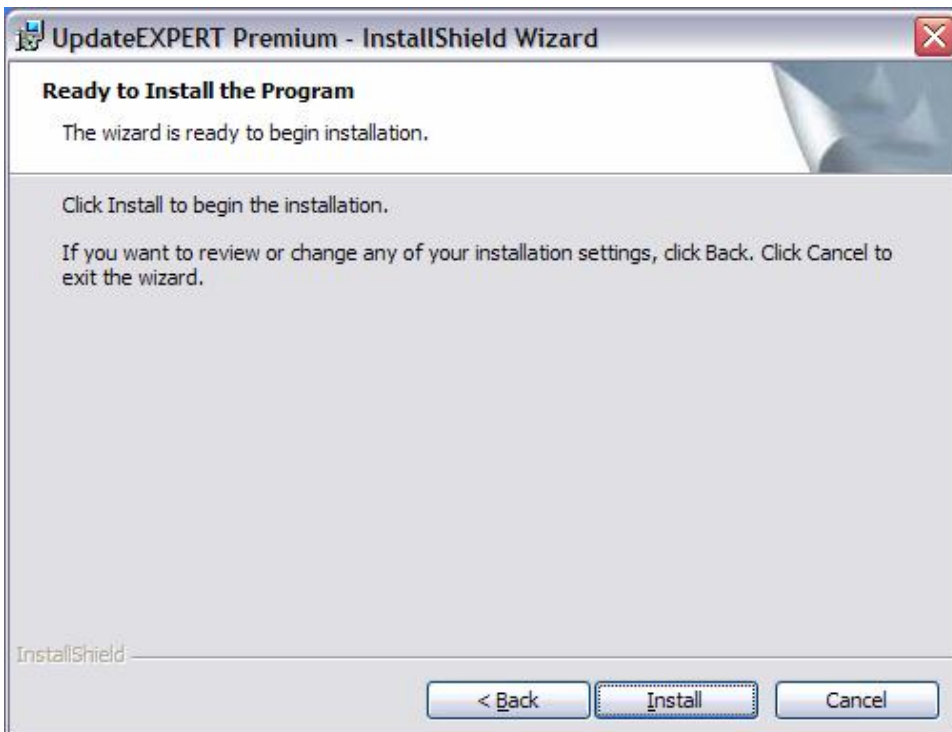
Enter the Trial Serial Number from the email called “**UpdateEXPERT Download Request.**” You may also request a trial serial number using the button shown below to launch a web form.



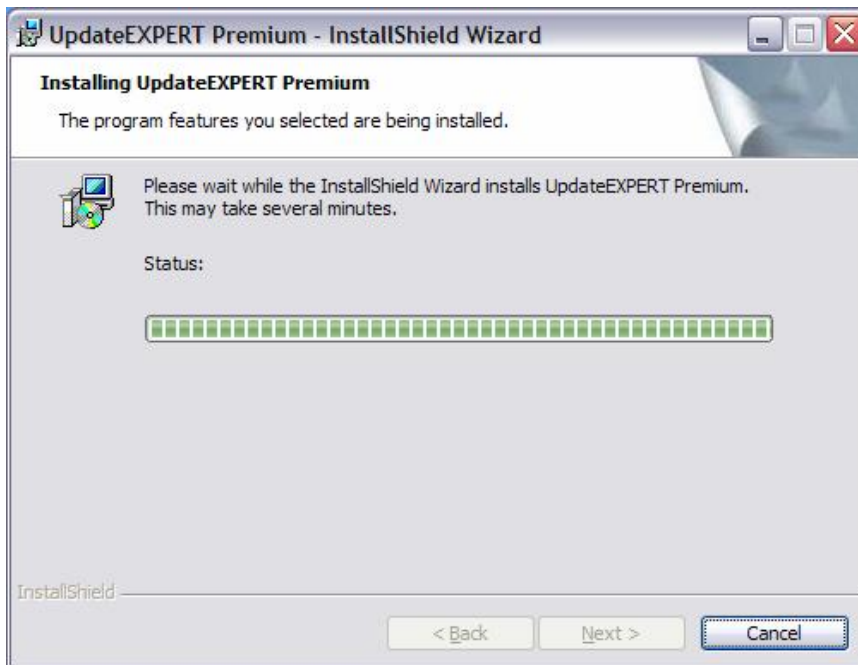
Typical will install all components, i.e., *Console Application, Patch Management Server* and *Settings Management Server*. **Custom** may be used to install to an *existing Local SQL instance*, exclude “Settings Management”, or install the Console and Agent-Installer Applications only. For example screen shots and notes, see “[Appendix A – Custom Install Options](#).”



Click **Install**



You will see a “**Performing Initialization Check ... Please Wait**” message. In 1-2 minutes status messages and the status bar will become active. UpdateEXPERT and MSDE files are loaded ...



File Loading results in 3 UpdateEXPERT directories...

1. C:\Program Files\St. Bernard Software\UpdateEXPERT
2. C:\Program Files\Common Files\UpdateEXPERT
3. %Systemroot%\UEAgent

Note: %Systemroot% will be C:\WINNT or C:\WINDOWS.

... and creation of an MSDE directory, or use of an existing SQL directory:

- C:\Program Files\Microsoft SQL Server\MSSQL\$SBSDB or MSSQL\$LocalSQLInstance

Note: The Master Agent is started automatically... look for **UEAgent** in task-manager, or the services list. There are also several child processes spawned by UEAgent, their names all start with "UE" such as **UEFile**, **UELog** etc.

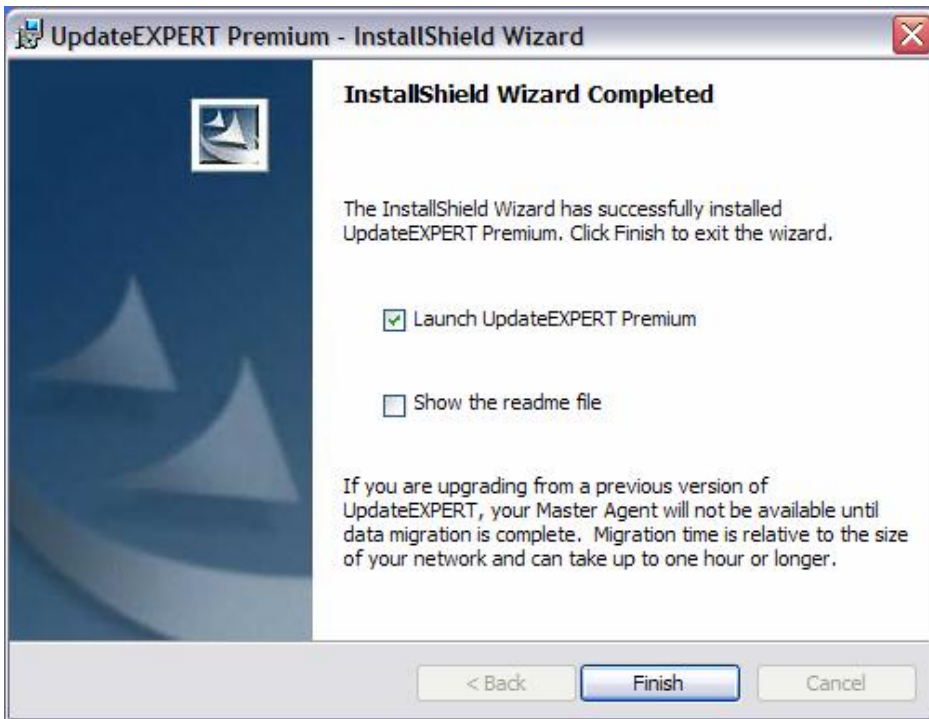
Patch Targets use this working directory during patching:

- %Systemroot%\ue_installs

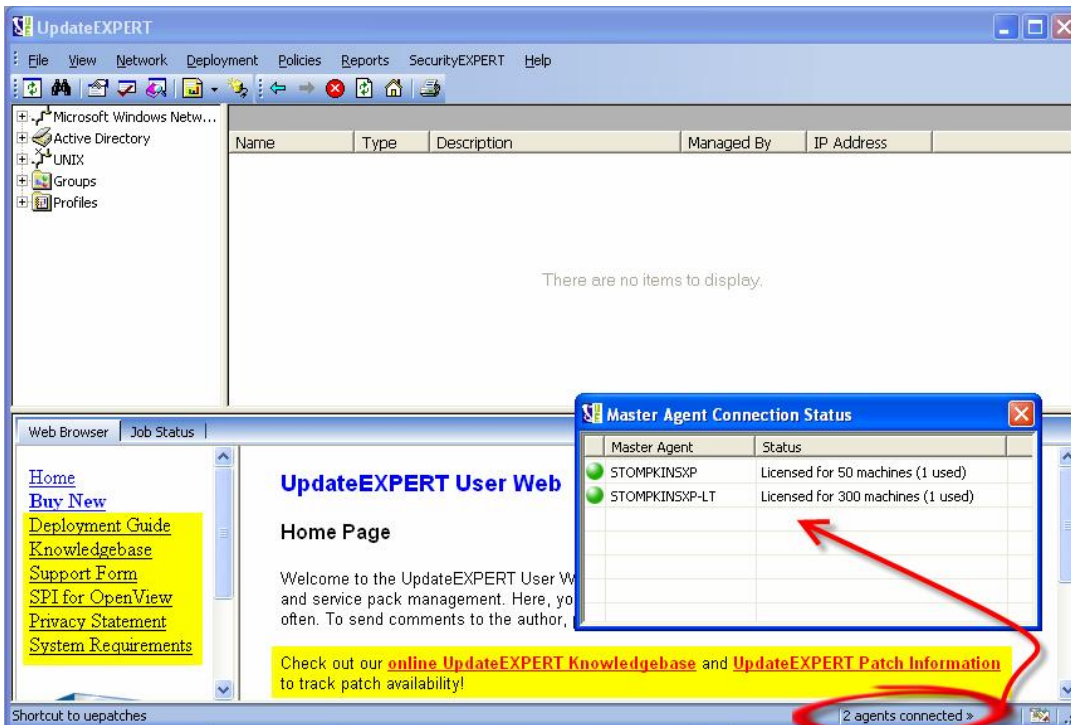
If Settings Management is included, there will be 3 Settings Management directories, and they will be mapped as Virtual Directories in IIS:

1. C:\inetpub\wwwroot\SecurityEXPERT
2. C:\inetpub\wwwroot\SEServerWS
3. C:\inetpub\wwwroot\SBSCorporateClientWS

Launch UpdateEXPERT ... click Finish



Double-click the 'agents connected' message on the status bar to see connected agents (1 at this point). Below, two connected Master-Agents are shown as an example of multiple connections. **Note:** If you didn't login with Administrative rights, you may be prompted for credentials. The display areas include **Network Pane** (upper-left), **Updates Pane** (upper-right), and **Browser Pane** (bottom). The **Job Status Tab** allows viewing job and task history information.



Note: When you deploy additional Master-Agents (using **File > Agent > Install Wizard**) you can connect to them using **File > Agent > Connect/Configure**. Additional Master-Agents are typically deployed for delegation or scaling reasons.

The **Network Pane** (upper-left) is where you “discover” machines, simply by expanding the **Window Network** or **Active Directory** objects. These views are identical to viewing your network from “Network Neighborhood”. Unix machines can also be discovered with “Network > IP Scan”, and added to the **UNIX** object. IP Scan works for Windows machines also, but they are added to the Domain tree. **Groups** and **Profiles** are empty till you create a Group, or run the Profile Wizard. See “**Help > Contents**” to access the online User Guide for more information.

The **Updates Pane** on the right (empty on initial launch, as shown above) populates with machine-specific patch information (installed & not-installed patches) when you Query one or more machines. **Note:** [configure your Web Proxy](#) (next topic), then [Download the latest database](#) before querying target machines for a meaningful and accurate patch inventory.

The **Web Browser** tab (shown on prior page) displays:

- Announcements (upgrades, etc.)
- Link to the “UpdateEXPERT Knowledgebase”
- Link to the “Patch Information Database”
- KB Articles for Windows, Solaris, RedHat Linux platforms
- HTML reports

Links on the left (shown on prior page) allow:

- Checking your subscription
- Downloading the **Deployment Guide** (more detail on Agent Architecture)
- Submitting support requests with a form

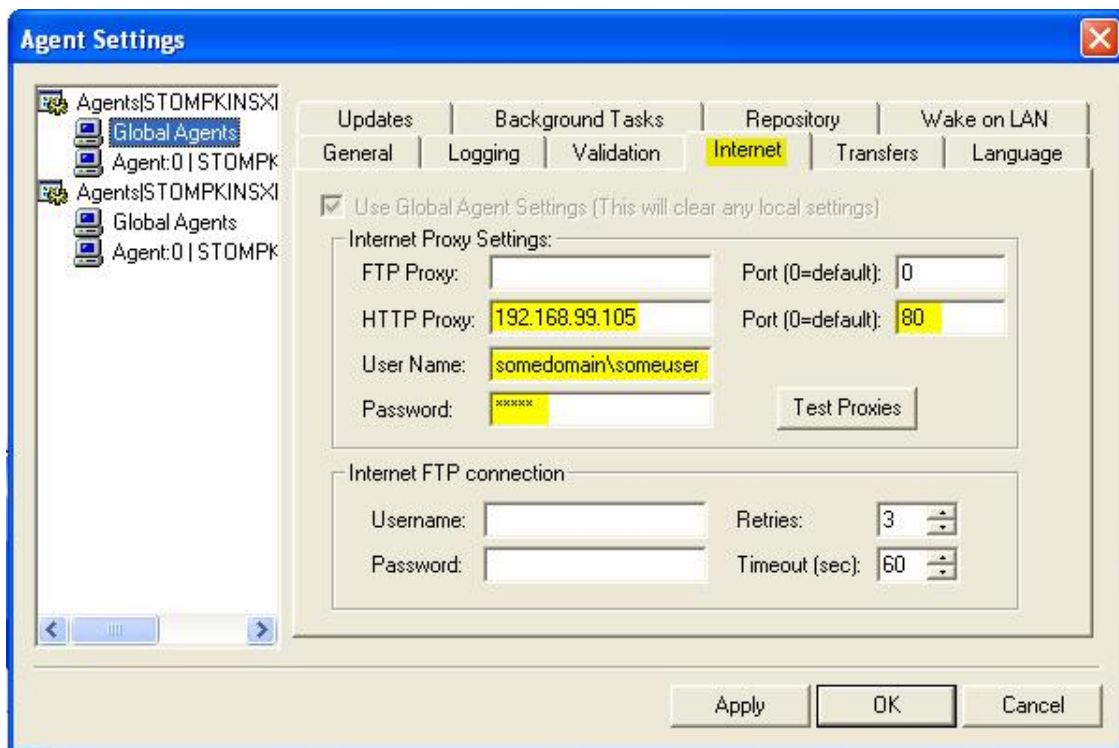
The **Job Status** tab allows display of UpdateEXPERT event history. This is a 3 level drill-down. At the top level one or more Master-Agents are listed. Next/Back allow drilling-down to Job Statistics and Task Statistics levels for details about various operations. All status information can be deleted from Job Status tab. Machine specific status information can also be deleted from the Deployment Status window.

Job Statistics							
Job Type	Status	Total Machines	Succeeded	Failed	Create Time	Start Time	
Query	Success	1	1	0	08/16/05 17:18:21	08/16/05 17:18:21	▲
Query	Success	1	1	0	08/16/05 17:28:41	08/16/05 17:28:43	
Query	Success	1	1	0	08/16/05 17:46:10	08/16/05 17:46:10	
Query	Failed	1	0	1	08/16/05 17:47:24	08/16/05 17:47:28	
Query	Failed	1	0	1	08/16/05 17:47:49	08/16/05 17:47:50	▼

Identify the Web Proxy (if applicable)

If your organization uses a Web Proxy Server you need to identify it so that UpdateEXPERT can successfully submit URL requests to St. Bernard and Microsoft web sites for database updates, and patch downloads.

Navigate to "**File > Agent > Settings > Internet**" and identify your web proxy server. It is best to enter the information for the "Global Agent". The **Global Agent** represents default settings applied automatically to a Master-Agent and all of its Leaf-Agents.



As browsers have evolved, the FTP settings have become "legacy" items that don't usually need to be specified. **Test Proxies** button is useful for testing internet access.

Note: The following URL's must NOT be blocked by a Web Proxy or by a Firewall, for successful UpdateEXPERT database/product updates. This is usually not an issue but is mentioned just in case there are firewall or web filtering restrictions in your environment. You'll receive a download error message (see the next section) if firewall restrictions are preventing a database update.

<http://www.stbernard.com>
<http://ueupdates.stbernard.com>
<http://patches.stbernard.com> (for **RedHat** Linux patch downloads only)

If firewall issues persist, see [Internet Firewall Requirements](#) for more tips.

Download the Latest UpdateEXPERT Database

Do **“Help > Update Database Now”** and *wait at least a minute* for a dialogue box to come up asking if you want to update your database. Click Yes to update (actually replace) the existing database files with new database files immediately, or simply wait for the countdown timer to expire



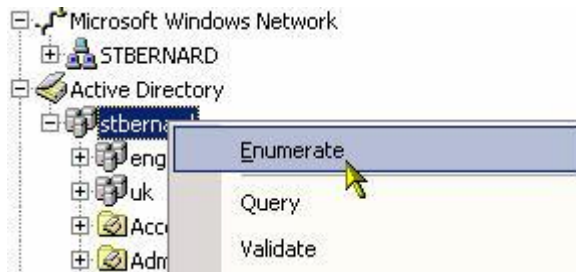
After this initial database update, UpdateEXPERT will automatically check for a new database every 6 hours by default. You may reconfigure this by going to **“File > Agent > Settings > Updates”** and changing the scheduling of the automated database check.

Confirm you have the latest database and product build by looking for ["Current UpdateEXPERT Database: XXXX"](#) on the *database Information web page* maintained by St. Bernard Software. This information is updated frequently by our internal Tech-Support staff, informing the UpdateEXPERT community about recently added patches to the UpdateEXPERT database. You can "bookmark" this location to help during "Patch Tuesdays" (Microsoft's monthly security patch releases). A link is also available in the UpdateEXPERT User Web frame.

If there is a Web Proxy, Firewall, or some other connectivity issue, you will likely get the message **"Unable to request update information from St. Bernard Software"**. Please contact your internal network support staff for assistance and provide them with the URLs that must not be blocked. and ultimately UpdateEXPERT Tech-Support if the issue persists.

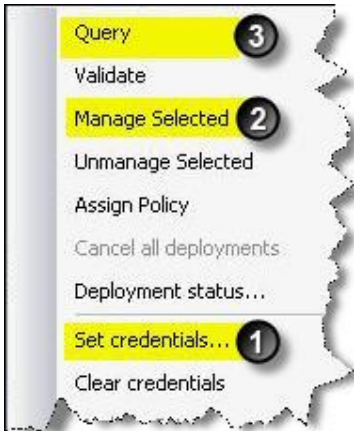
Enumerate (Discover) Machines

Enumerate your network by expanding the **"Microsoft Windows Network"** to see your domains. Expand the domain with your UpdateEXPERT machine in it. Expanding the network objects initially populates the network tree. In the future you can Enumerate-on-demand to pick up newly added hosts, as shown below. The command is available (right-click) at the **Domain** and **OU** level, and the **network object level** (for example, Active Directory). You may delete domains or machines from your view with right-click > Delete. You may also use **“View > Machine Filter”** for defining machine display criteria (name, agent type, etc.) These settings are saved on a per-user basis.



Query your UpdateEXPERT Machine

Begin by querying a machine you have Administrative rights on, i.e., your UpdateEXPERT Master-Agent machine, as a means of testing and learning. Select (highlight) your UpdateEXPERT machine, **right-click**, do **1) "Set credentials..."** and enter valid credentials. Then do **2) Manage Selected** (decrements license count). The machine name will **bold** and means the machine is eligible for querying and patch deployment. Then do **3) Query** to get a patch inventory. **Note:** a Globally Unique Machine-ID ("GUID") is written to the target machine when you "manage" it. If you get prompted for credentials using "Manage Selected" it is because you have not used "**Set Credential**" at the domain/AD container level, or the machine level yet, or the credentials are invalid. Enter admin credentials when needed, and the Machine ID will be written. Then do the Query command again.



Next, see "[Icons](#)" quick reference to quickly get familiarized with UpdateEXPERT icons. Use the application **Tabs** (below) to see how patches are grouped, click any of the **column headers** for sorting. Patches are sorted by **Release Date** (new to old) by default. Sorting on the "balloons" (**Green** Balloons represent installed patches. **Grey** Balloons represent uninstalled patches.), or patch type (see "key" icons below for security patches) are useful, for example.

Windows XP Professional (English (United States)) - Service Pack 2									
All OS Browsers Exchange SQL Server IIS Media MDAC Outlook Office ISA XML Web Services 1 4									
	Name	KB Article	Description	Release Date	Install Date	Platform	Langu...	Repository ID	
	WindowsXP-KB...	Q901214	[MS05-036] V...	7/12/2005 12:...	7/18/2005	Windows...	English ...	0x00002c2d	
	WindowsXP-KB...	Q898461	Update for Wi...	6/27/2005 12:...	7/18/2005	Windows...	English ...	0x00002c09	
	WindowsXP-KB...	Q900930	An update tha...	6/24/2005 12:...	Not Installed	Windows...	English ...	0x00002be7	
	WindowsXP-KB...	Q884883	Multiple versio...	6/17/2005 12:...	Not Installed	Windows...	English ...	0x00002be6	
	WindowsXP-KB...	Q896428	[MS05-033] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002aec	
	WindowsXP-KB...	Q890046	[MS05-032] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002afc	
	WindowsXP-KB...	Q896422	[MS05-027] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002af0	
	WindowsXP-KB...	Q896358	[MS05-026] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002af6	
	WindowsXP-KB...	Q893066	[MS05-019] V...	6/13/2005 12:...	5/10/2005	Windows...	English ...	0x00002afa	
	WindowsXP-KB...	Q894391	FIX: DBCS att...	5/18/2005 12:...	Not Installed	Windows...	English ...	0x00002a48	
	WindowsXP-KB...	Q896626	Windows XP T...	5/13/2005 12:...	Not Installed	Windows...	English ...	0x00002a31	
	Windows Insta...	MsInstall...	Windows Inst...	5/12/2005 12:...	5/4/2005	Windows...	English ...	0x00002a32	

When you wish to query more machines, you will need to select a domain/AD container, or one or more individual machines, and use **Set Credential** to specify a domain or local machine administrative account that will allow you to query.

Agentless Query Requirements

These requirements are the result of default installations for NT4/W2K/XP. You would have to disable these services and shares, and restrict access, to fall short of the requirements. In order to install OS updates remotely you must have the access rights to remotely access and modify the registry and system files on the target systems.

Administrator Account (Domain or Local) with administrator rights on target machines

Required Services, in addition to the baseline RPC Service (Console and Target machines):

**Remote Registry
Server
Netlogon
File and Print Sharing (NIC configuration)**

Share Access:

Admin\$ - enabled and accessible by UE account

IPC\$ share - enabled and accessible by UE account

Admin shares for other drives whose installed components may be queried.

Remote Registry Access – "Full Control" permission to target machine registry.

The account used for access must have Full Control remote access to the registry of the target system. You must be able to open the remote registry of the target system in REGEDT32 on the UpdateEXPERT Console Machine. This procedure will confirm remote registry access and access to IPC\$:

1) Launch REGEDT32 on the UpdateEXPERT Console Machine. Choose "Registry-Select Computer" and enter the name of the target system. In this remote registry, go to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

2) With the above key highlighted, choose "Security-Permissions" from the top menu. You must be a member of the group that has Full-Control access to this key and its subkeys to successfully Query a system.

Windows XP/2003 Remote Login Access policy must be set to "Classic" mode: Go to **Start > Programs > Administrative Tools > Local Security Settings > Local Policies > Security Options** and click the "**Network access – Sharing and Security Model for Local Accounts**" item. Change the policy to the "**Classic**" selection. This allows a remote login to remain themselves instead of being mapped to the guest account.

Windows XP/SP2 tightens security. Please see this [XP/SP2 article which tells you how to configure the firewall](#) to allow queries (of course, you can turn off the firewall on the client side if you wish, temporarily or permanently).

For more detail on the issues above, [click here](#).

Download Patches

Note: Patches which are not downloaded already, are automatically downloaded by the Patch Install Wizard. Here we do it manually primarily as a learning exercise.

Select (highlight) one or more uninstalled patches, right-click and “**Download**”. Diskette Icons will turn **blue** with a **red arrow** while downloading, and will turn **solid blue** (shown below) when successfully downloaded. **Grey** means not downloaded.

Name	KB Article	Description	Release Date	Install Date	Platform	Langu...	Repository ID
WindowsXP-KB...	Q901214	[MS05-036] V...	7/12/2005 12:...	7/18/2005	Windows...	English ...	0x00002c2d
WindowsXP-KB...	Q898461	Update for Wi...	6/27/2005 12:...	7/18/2005	Windows...	English ...	0x00002c09
WindowsXP-KB...	Q900930	An update tha...	6/24/2005 12:...	Not Installed	Windows...	English ...	0x00002be7
WindowsXP-KB...	Q884883	Multiple versio...	6/17/2005 12:...	Not Installed	Windows...	English ...	0x00002be6
WindowsXP-KB...	Q896428	[MS05-033] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002aec
WindowsXP-KB...	Q890046	[MS05-032] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002afc
WindowsXP-KB...	Q896422	[MS05-027] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002af0
WindowsXP-KB...	Q896358	[MS05-026] V...	6/14/2005 12:...	Not Installed	Windows...	English ...	0x00002af6
WindowsXP-KB...	Q893066	[MS05-019] V...	6/13/2005 12:...	5/10/2005	Windows...	English ...	0x00002afa
WindowsXP-KB...	Q894391	FIX: DBCS att...	5/18/2005 12:...	Not Installed	Windows...	English ...	0x00002a48
WindowsXP-KB...	Q896626	Windows XP T...	5/13/2005 12:...	Not Installed	Windows...	English ...	0x00002a31
Windows Insta...	MsInstall...	Windows Inst...	5/12/2005 12:...	5/4/2005	Windows...	English ...	0x00002a32

The diskettes will turn **orange** if the download fails. This is typically a proxy or firewall issue if the problem persists. By default, patches are downloaded to `%systemroot%\UEAgent\Download` and given a unique Repository-ID that can be easily cross-referenced to the Microsoft name using the **Name** and **Repository ID** columns in the UpdateEXPERT interface (shown above).

The download Repository can be re-configured (**File > Agent > Settings**) to be a non-boot drive (D: for example), or a network share (UNC syntax only, not mapped drive letters).

General | Logging | Validation | Internet | Transfers | Language
 Updates | Background Tasks | **Repository** | Wake on LAN

Use Global Agent Settings (This will clear any local settings)

Location: [NTFS volume is recommended]

Credentials (remote location only)

Domain:

User name:

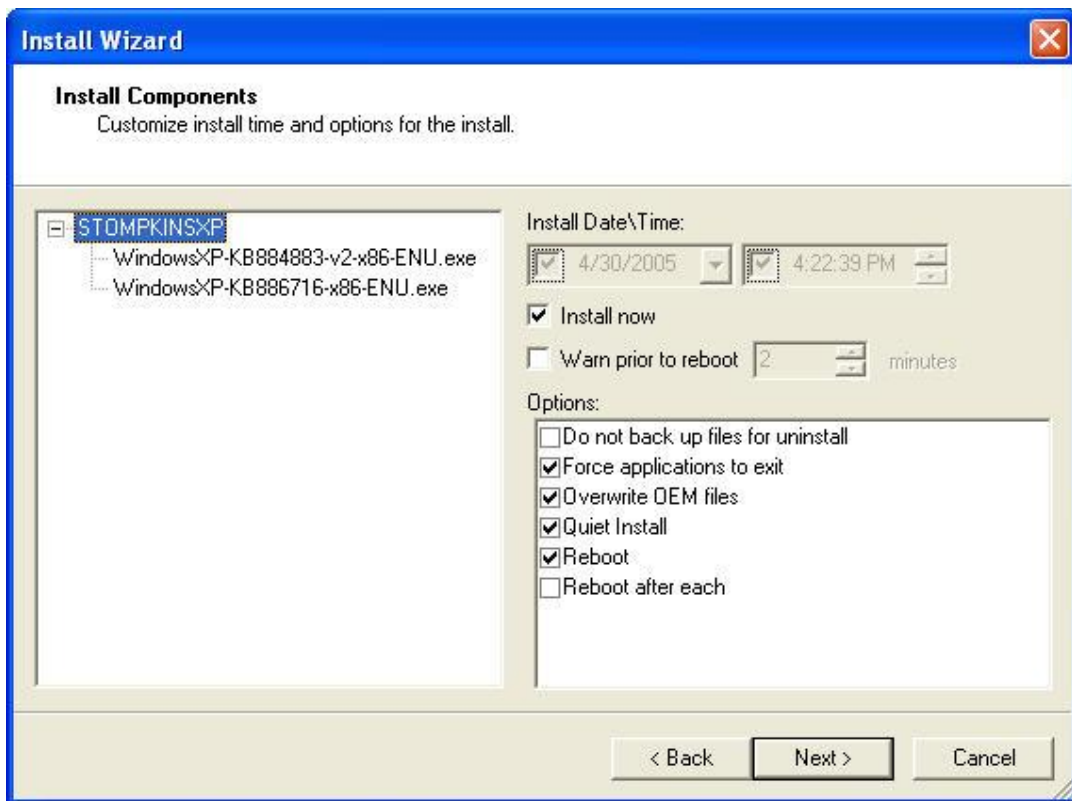
Password:

Confirm password:

Install Patches

Suggestion: For the moment, install patches on your UpdateEXPERT machine. Later, you can deploy to other machines.

Select (highlight) one or more uninstalled patches, right-click and “**Install**”. This will launch the **Patch Install Wizard**, which integrates with the database for grouping patches, presenting [patch options](#) (see below), displaying diagnostic patch deployment messages, and controlling reboots. Set an install time a few minutes in the future (uncheck “Install Now” and set the minutes value ahead).



When you “Finish” the wizard, patch installation instructions, the persistent installer, and the patches themselves are transferred to `%systemroot%\ue_installs` on the target machine.

When the transfer is complete, the “**Deployment Status**” command will show **Pending**. Also, there is a **Job Status** Tab where a history of UpdateEXPERT events is kept per Master-Agent.

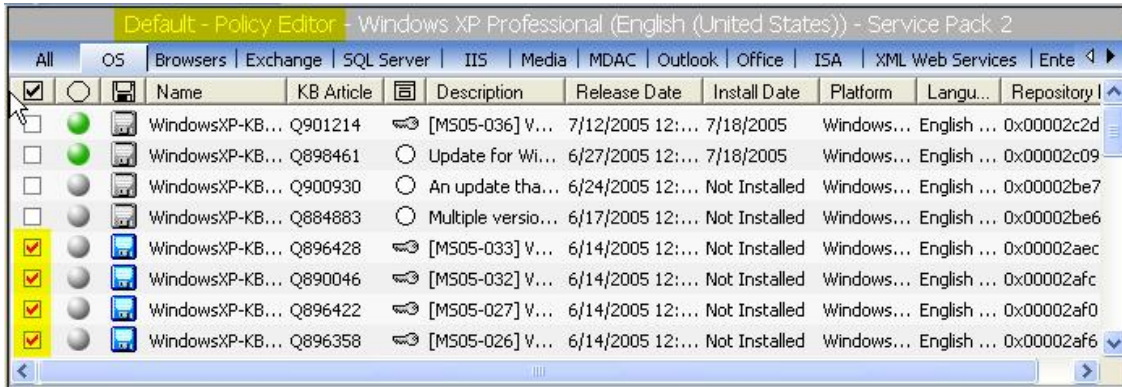
Note that the files in ue_installs are deleted after the installation, and the installation service uninstalls itself, leaving a clean machine. This logic applies to Leaf-Agent targets also, except that the installer service file permanently resides on the Leaf-Agent machine. Deployment Status or Job Status will now show **Completed**, or possibly an error if there was an issue.

Now query the machine again and verify the patches are installed (green balloons).

Note: It is always recommended (for this evaluation, and as a general rule) that all patches be tested before deployment in the production environment.

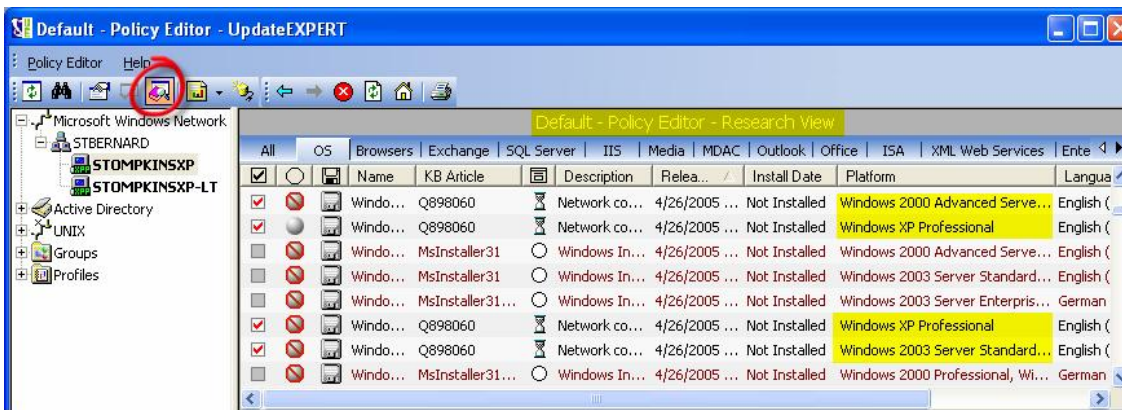
Named Policies (“Install Required” command)

To get started, select your UpdateEXPERT machine and open the Policy Editor for the Default policy as follows; **Policy > Open > Default > Open**. You may now check one or more patches as required (example below). At this point, you should be in the Policy Editor for “Default”, as shown below. Checking an update makes it “global” in the sense that it will update all applicable machines (ignoring non-applicable machines) when you do **Install Required**. **Policy > New** lets you create additional named policies if you wish. Once policies are created and saved (Policy Editor > Save), use right-click > **Assign Policy** to associate a named policy to your machine.



Before deploying required updates, let’s run a conformance report to see if your machine is “out-of-compliance” (as it should be, until patched). Basically, we need to 1) “check” an update for the **Default** Policy (and save it), 2) assign the Default policy to the machine, 3) configure Conformance Report options, and 4) run the report. So, pick a “not-installed” patch for your machine, check the patch in the Policy Editor in either machine or **Research View** (as explained next), and assign the Default policy to your machine. Then see Conformance Reporting (below).

With your machine selected, do **View > Research View** or click the button circled below, to switch to Research View, which is a list of every patch available in the UpdateEXPERT database. Required Updates can be specified here also. Most patches apply to multiple platforms. When you check/uncheck the patch, multiple line items will be automatically checked/unchecked for you, for multiple platforms. Below, as an example, we selected **898060** for Windows XP (yellow). Unchecking any one of them unchecks them all.

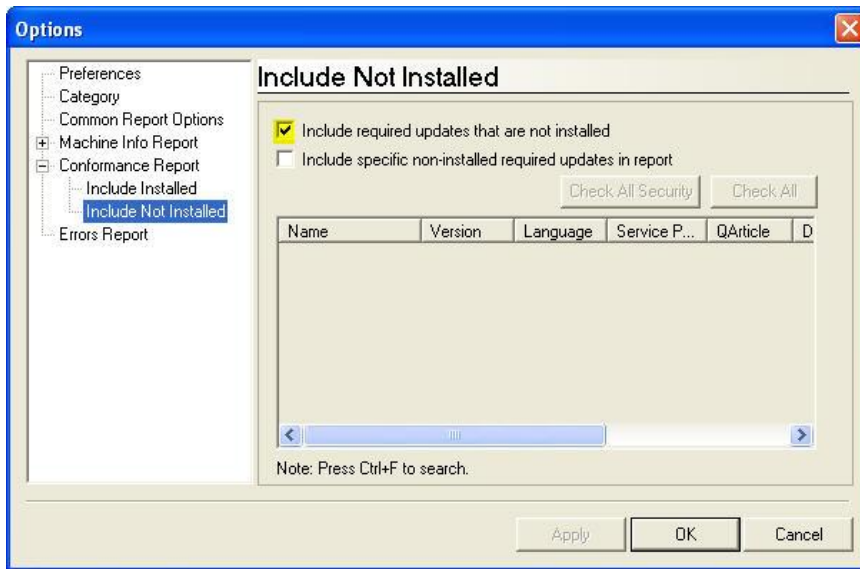


Note: Use the Checkmark button to filter-out all but the checked items. Go back to the machine detail view by de-selecting the button circled above (the button highlight goes away).

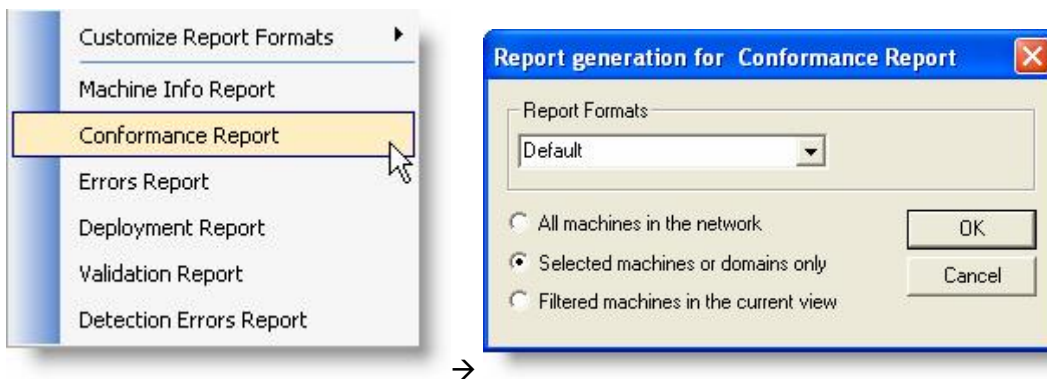
Conformance Reporting

Conformance Reporting tells you whether Required Updates have, or have not, been installed on specific machines. You can, for example, deploy a required update, re-query the machines, and run a Conformance report to see if any machines were missed (these could have been offline for example, or unreachable because of hardening).

To check the Conformance Report configuration, go to **View > Options > Conformance Report > Include Not Installed**, and verify that **“Include required updates that are not installed”** is checked (as shown below). Make sure **Include Installed** options are un-checked. This will simplify the report for evaluation purposes.



Go to **Reports > Conformance Report** and run the report for your selected machine.



You should get output similar to below in the **Web Browser** tab of UpdateEXPERT.



Select only your machine, right-click and **Install Required** to deploy required updates to all selected machines (yourself at this point). This will launch the **Patch Install Wizard** again. Click through the dialogue to install the required updates on your machine. Re-run the conformance report, your machine should NOT show up under “Does Not Conform”.

Note that you may export a combination machine/conformance report to CSV format with File > Export. This is explained in more detail below. Finally, an important reporting benefit in UpdateEXPERT Premium is the ability to aggregate data from Multiple Master-Agents. This lets you produce a single conformance report while connected to 2 or more Master-Agents.

Other Reports

Note: The console aggregates report data from all connected Master-Agents. This consolidated data can also be exported with **File > Export** (see below).

- The **Machine Info Report** provides a list of managed/queried machines and the updates installed and not installed on them.
- The **Conformance Report** provides a list of the machines that do and do not conform to the Required Policy. It lists the patches from the Policy that are missing and present on the machines.
- The **Errors Report** provides information on any query errors.
- The **Deployment Report** provides information on deployment status, start times, stop times, and any deployment or installation errors.
- The **Validation Report** will provide a list of machines and their patches with validation problems.
- The **Detection Errors Report** provides information on any patch detection problems.
- **"File > Export"** combines Machine and Conformance into a single CSV output file that can then be manipulated in for reporting purposes, or imported to a SQL database for the same reason. Administrators managing different networks or network regions can run a CSV report, give it a standard name like "machinename_mmddyy.csv", and place it in a central collection point where it can be imported into SQL, basically creating a patch history for target machines.

Installing Master or Leaf-Agents

The Agent-Installer GUI makes it easy to deploy additional Master-Agents, or Leaf-Agents to another machine. Do **File > Agent > Install Wizard**. 3 screens prompt for the needed information.

The screenshot shows the 'Agent Install Wizard' dialog box with the title 'Local/Remote Agent Installation'. The main question is 'Do you want to install this agent locally on this machine or remotely to another machine in the network?'. Below this, there are two radio buttons: 'Local' and 'Remote'. The 'Remote' option is selected. To the right of the 'Remote' radio button is a 'Serial Number' field with a blacked-out value. Below that, there is a text box for 'Host' containing 'MYTARGETMACHINE'. A 'Port' field contains '9968'. A 'Description' field contains '<<Agent Description>>'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

The 1st screen specifies a remote install (push the agent across the network) to a machine called "MYTARGETHOST". The port will be 9968 (the default) and we'll take the default description of Hostname|Type (meaning Master or Leaf-Agent)

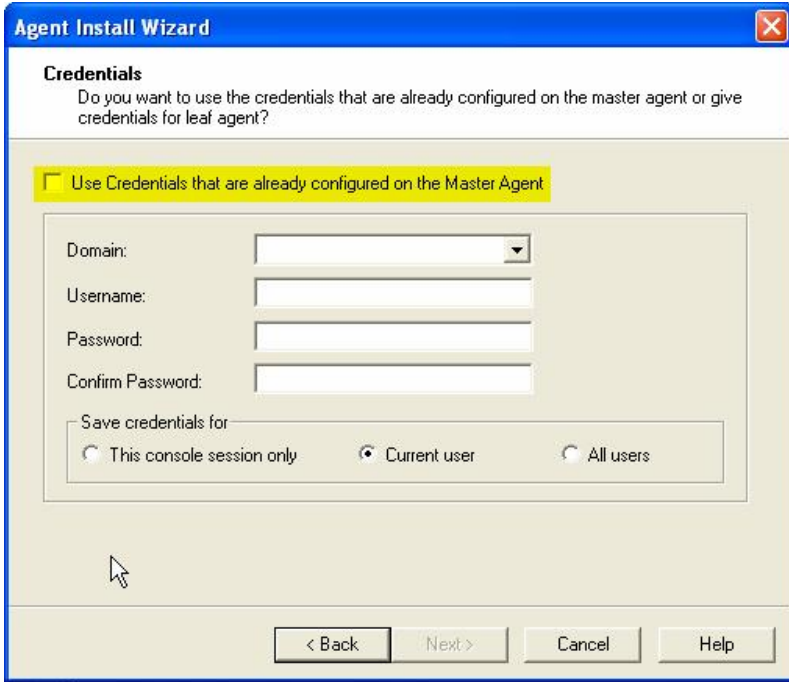
Note that port number must fall in the range of **1025 – 65535** if you change from the default.

You may use **IP-Address** in place of hostname if you wish (for static IP assignments on Servers for example).

The screenshot shows the 'Agent Install Wizard' dialog box with the title 'Master/Leaf Agent Installation'. The main question is 'Do you want to install this agent as a Master agent or Leaf Agent?'. Below this, there are two radio buttons: 'New Install' and 'Reinstall/Upgrade Agent (retain settings)'. The 'New Install' option is selected. Below that, there are two radio buttons: 'Master' and 'Leaf'. The 'Leaf' option is selected. Below that, there is a text box for 'Host' containing 'MYUPDATEEXPERTHOST'. A 'Port' field contains '9968'. An 'Instance' dropdown menu is set to 'Create SBSDB'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

The 2nd screen says the Agent is "new" (as opposed to a re-install or upgrade), and that it will be a Leaf-Agent. We specify who the Master-Agent host is so the Leaf-Agent can register with the Master. We'll use port 9968 again so only one port needs to be opened on any intermediate firewall.

Notes about port and IP from above apply to this screen as well.



The 3rd screen lets you use existing “**Credentials**” to perform the remote installation, or lets you specify credentials as needed.

Also note that the specified credentials can be saved for the session only if your policy prohibits storing credential information.

When you click “Finish”, the Leaf-Agent will be pushed, and status information displayed. At the end of the dialogue you will be notified of success. A “**head**” icon (highlighted below) indicates an installed Leaf-Agent (see below). Allow a few minutes for starting the Leaf-Agent service and updating the database. You may get “Unable to Connect” until the Leaf-Agent is ready.



Once you have a Leaf-Agent target, go ahead and query the machine and deploy patches to it if you wish. Installing Leaf-Agents doesn’t change the patch deployment logic in any substantial way, making it easy to work with a mix of Agentless and Leaf-Agent machines.

In summary, Leaf-Agent installation options include:

- | | |
|-------------------------|---|
| Remote | (non-hardened targets ... as shown above) |
| Local | (hardened targets ... you can install just the Agent-Installer, see Custom Install) |
| Command-Line | (Mass Deploy) |
| Active Directory | (Mass Deploy) |

See this [When Should I Deploy Leaf-Agents?](#) for more information. Please contact Tech-Support for questions or assistance.

You have now been exposed to setting credentials for Managing, Querying and Agent Installation. For a very complete discussion of how credentials are stored and managed, see:

[Credentials Management in UpdateEXPERT Premium](#)

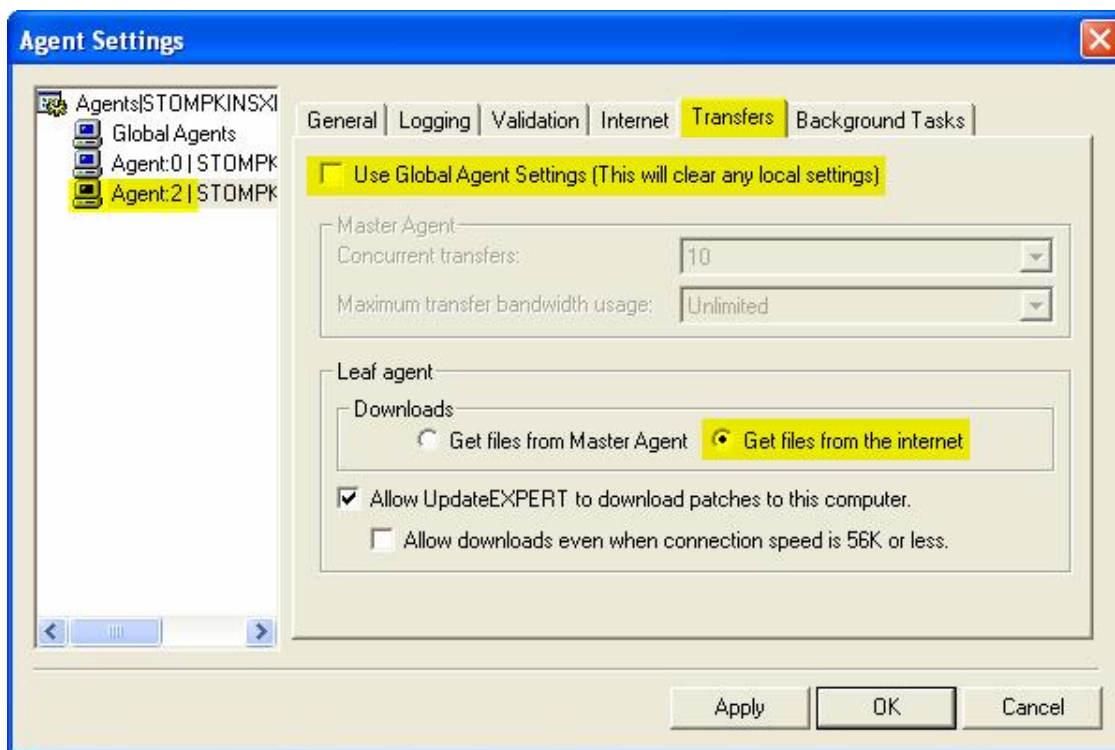
Lastly, it is highly recommended you review the Leaf-Agent [Deployment Guide](#). This document reviews Master and Leaf-Agent Architecture.

Leaf-Agent Configuration

Leaf-Agents support a subset of the available Master-Agent Tabs (6 of 10 tabs currently) in **File > Agent > Settings**.

Using these Tabs, Leaf-Agents can be configured for background query, logging level, and depth of validation. Leaf-Agents can also be configured to download patches from the internet (shown below), and gain internet access through a web proxy server.

Note that the **Master-Agent** is always **Agent:0**. **Leaf-Agents** will be **Agent:2** and higher. The Leaf-Agent uses **Global Agents** defaults, unless you specify otherwise by un-checking "Use Global Agent Settings" checkbox shown below.



What's Next?

Congratulations! You've used important core UpdateEXPERT features. See **Help > Contents** (User Manual) for information on creating **Groups** and **Profiles**. Profiling in particular is a great way to group machines by OS, Service-Pack, Applications, and even individual patch.

See "[What's New in UpdateEXPERT Premium](#)" to see a menu of features that were introduced in UpdateEXPERT Premium.

You may also want to deploy a **Custom-Fix** ... See "[Why would I use Custom-Fixes?](#)".

If interested in **Unix** support, please see "[Getting Started with RedHat and Solaris](#)".

The remainder of this Evaluation Guide (below) discusses several more Patch Management functions:

Validation

Scheduling Queries

Logging

... and is followed by an introduction to "Settings Management" (a.k.a. **SecurityEXPERT**).

Validating Patches

Validation is supported by the UpdateEXPERT database. Validation examines file version, size, or checksum values in the database against individual component files of each installed patch on the target machine. If a mismatch on even one component file fails, Validation for that patch fails. The recommendation would generally be to re-install the patch, and to investigate if the user had recently installed software that may have overwritten a newer DLL (for example) with an older DLL. Select your machine, right-click and **“Validate”**. Note that Required Updates and Validation are supported for Unix targets.



The update has been installed and validated.

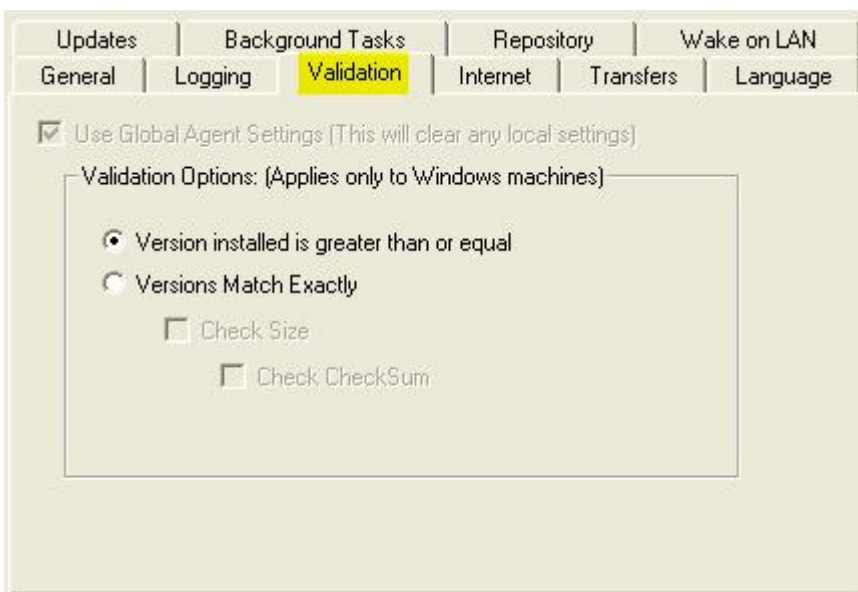


The update has been installed but the validation has failed.



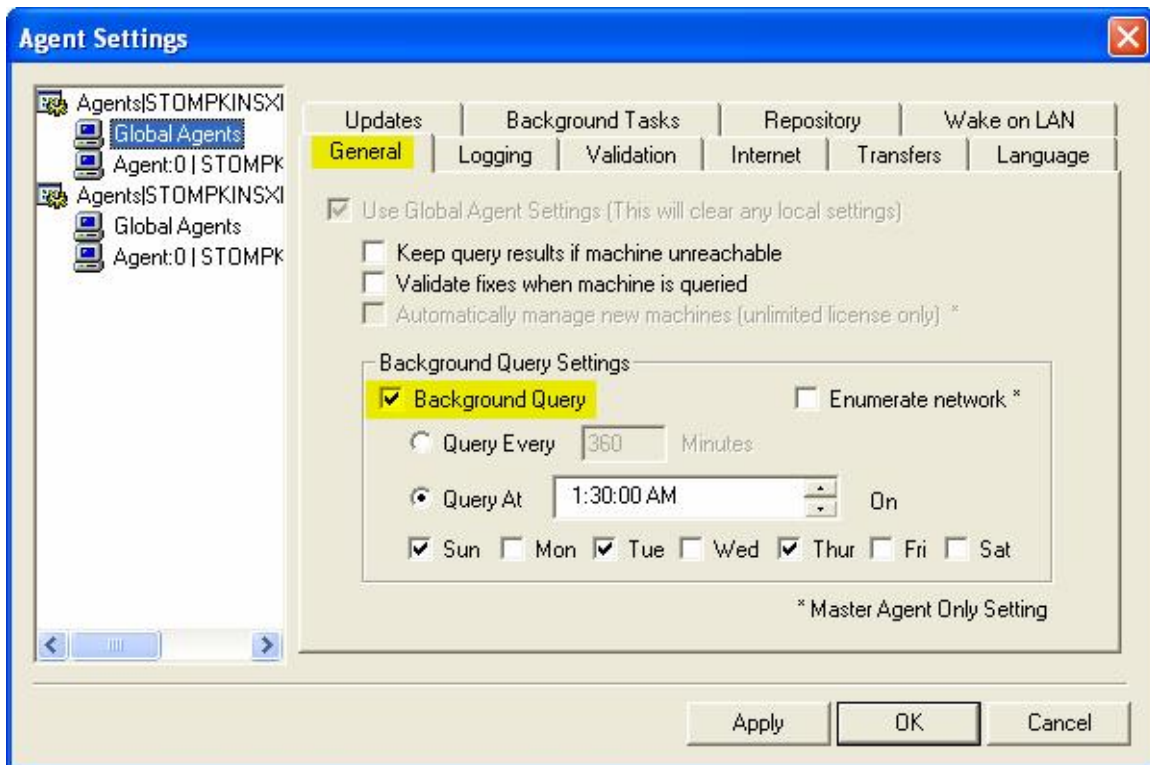
The update has been installed but there is no validation information available.

File > Agent > Settings > Validation allows configuring the depth of Validation. The default setting “Version installed is greater than or equal” is recommended to minimize overhead.



Scheduling Queries

Background **Enumeration** (to discover newly installed machines), **Querying**, and even **Validation** (**Note: query time increases substantially**), can be scheduled, such as during “off-hours”, for each deployed Master-Agent and Leaf-Agent. To apply a schedule to many Agents, it is best to select the **Global Agents** object. However, you can select any individual Agent, uncheck the “Use Global Agent ...” item, and configure a custom schedule for the Agent.



Above, for the Global Agent settings, which are inherited by subsequently installed Agents, we have specified Background Queries at 1:30 AM on Sunday, Tuesday, and Thursday. This might make sense for example, if I intend to install patches on Monday/Tuesday, Wednesday/Thursday and Friday.

Note that Agentless machines need to be queried by the Master-Agent. Installed Leaf-Agents can query themselves and report results back to the Master-Agent.

Above, Validate has not been checked off, and neither has Enumerate Network (which applies to the Master-Agent only, but these options are readily available).

Logging

Go to **File > Agent > Settings > Logging** to specify which events will be logged on Master and Leaf-Agent machines. The Log size is configurable. The logfile itself can be found at:

C:\Program Files\CommonFiles\UpdateEXPERT\ActorUserLog.txt

SecurityEXPERT Overview

Settings Management (**Services, Registry, File, and Security Policy** settings) is provided by downloading one or more security templates from the UpdateEXPERT **Security Templates Tab**, and using the settings management information to:

- **Create Policies**, i.e., research and select security points of interest
- **Test Compliance**, i.e., assess the status of machines
- **Enforce Policy**, i.e., implement settings changes to enhance security

Important: *The actual enforcement of settings policy can change registry items, file-system permissions, and services settings. **Settings changes can negatively impact applications and users. It is strongly recommended that you completely research and understand your chosen security points when creating policy, and that you first test enforcement on appropriate test platforms.** You must test the effects of enforcement on applications & users. In general, understand what you are doing and why, and be conservative. Deployed settings changes cannot be easily reversed or undone.*

Related to the point above, is that file-system permission enforcements currently replace permissions that currently exist on the target file(s). SecurityEXPERT will apply the specified permissions for the accounts listed and will remove any other account or permission. Again, test how the permission replacement may impact applications/users.

Note: SecurityEXPERT settings that affect remote access are displayed with a warning icon. Losing remote access will prevent patch management and settings management.

Assuming you included SecurityEXPERT during installation, using SecurityEXPERT requires the following:

- Downloading SecurityEXPERT Templates
- Researching Security Points and Creating Policy
- Assigning Machines to a Policy
- Assessing Machines by Policy
- Policy Enforcement

The example that follows creates a policy starting with an “expert” recommendation for a “desktop” XP machine. For the sake of simplicity, you will clear all the security points, and create a simple policy for two services. This allows rapid familiarization with the SecurityEXPERT workflow. Using expert recommendations would be appropriate for setting a security “baseline” for newly installed or imaged machines. For existing machines, careful construction of your own policy, adding specific items over time, may work best. The intention of this Evaluation is to get you started on using basic SecurityEXPERT features and workflow. See the UpdateEXPERT User Guide for more information on SecurityEXPERT.

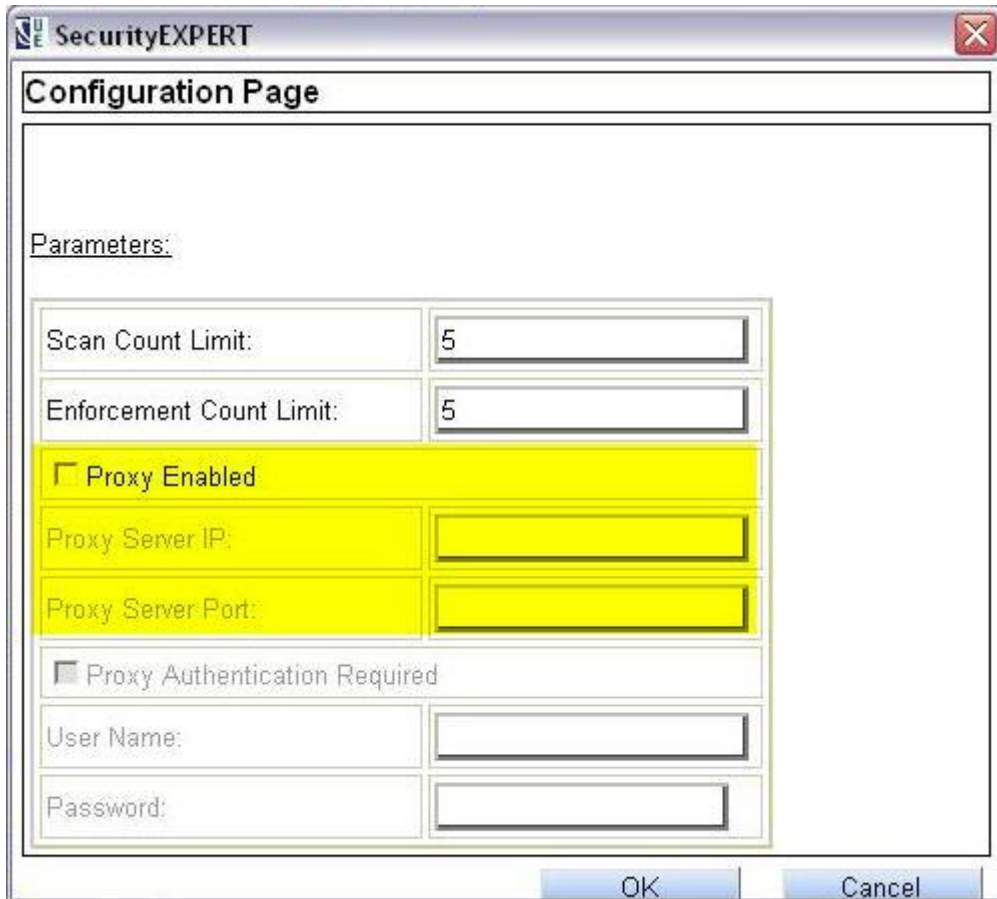
Configure SecurityEXPERT Web Proxy

Before attempting to download security templates, set Web Proxy settings if needed.

Settings Management is performed with a .NET interface accessed from UpdateEXPERT. This screen saves Web Proxy information to .NET configuration files. If you have identified a Web Proxy for UpdateEXPERT using **File > Agent > Settings > Internet**, you need to replicate those settings, or use other valid proxy settings so that security templates can be downloaded.

Go to **SecurityEXPERT > Options** to see the page below. At minimum you need to check "Proxy Enabled", then specify the "Proxy Server IP" and "Proxy Server Port" as highlighted below.

You may also enter Proxy *Authentication* information, if needed, after checking "Proxy Enabled".

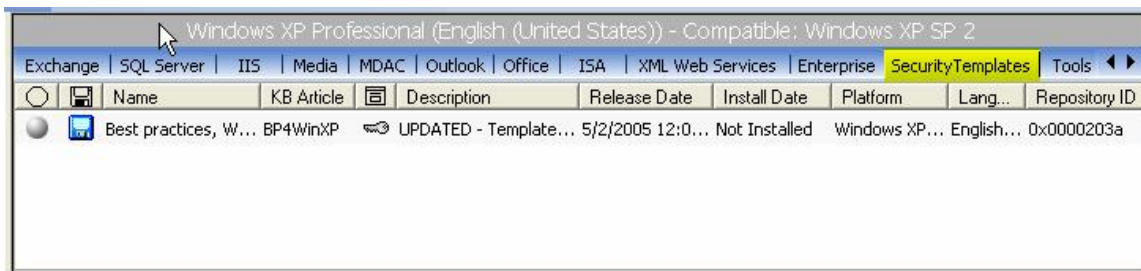


The screenshot shows a window titled "SecurityEXPERT" with a "Configuration Page" header. Under the "Parameters:" section, there are several input fields and checkboxes. The "Proxy Enabled" checkbox is checked and highlighted in yellow. Below it, the "Proxy Server IP:" and "Proxy Server Port:" fields are also highlighted in yellow. Other fields include "Scan Count Limit:" (5), "Enforcement Count Limit:" (5), "Proxy Authentication Required" (unchecked), "User Name:", and "Password:". The "OK" and "Cancel" buttons are at the bottom right.

Scan Count Limit:	5
Enforcement Count Limit:	5
<input checked="" type="checkbox"/> Proxy Enabled	
Proxy Server IP:	
Proxy Server Port:	
<input type="checkbox"/> Proxy Authentication Required	
User Name:	
Password:	

Download SecurityEXPERT Templates

New security templates are shown in the **Security Templates** tab (shown below) for queried machines. Templates may be seen in Machine (shown below) or Research View. Templates are available for Windows 2000 Professional and Server, XP Professional, and 2003 Server.



Go to the Security Templates tab for a queried machine, right-click the template, and “Download.” Downloading a template parses an XML data stream and writes new security point data to the configured MSDE or SQL database. Be patient, the templates contain a significant amount of data and may take longer than the average patch to download. **Blue** diskettes indicate the XML data stream has been written to the MSDE or MSSQL database on the SecurityEXPERT server (as shown above). You can serially download all templates using Research View (see notes).

Note1: It is always strongly recommended that you download one Security Template at a time. A template download error (**Orange** Diskette) will typically occur if attempting to download multiple templates. If a download error occurs, try again, downloading one template, then the next, etc.

Note2: In the future, if you see a **Grey** diskette for a template you know you already downloaded (i.e., it used to have a Blue diskette), this is an indication that a revised template has now become available. This usually implies the addition of new security points and should not affect existing policies, scans etc.

Once downloaded to the relational database, Security Templates are used to create user-defined policies, which are user specified security points to assess and potentially enforce.

Note that security points ...

- are sourced from well-known “experts” such as Microsoft and various security organizations. Different templates support different numbers of experts, hence security points, i.e., templates are not identical.
- may or may not apply to a certain machine configurations (which indicates type of usage) such as “Server” or “Laptop” or “Desktop Client.”

In summary, security points are determined by a combination of selected experts and machine configuration.

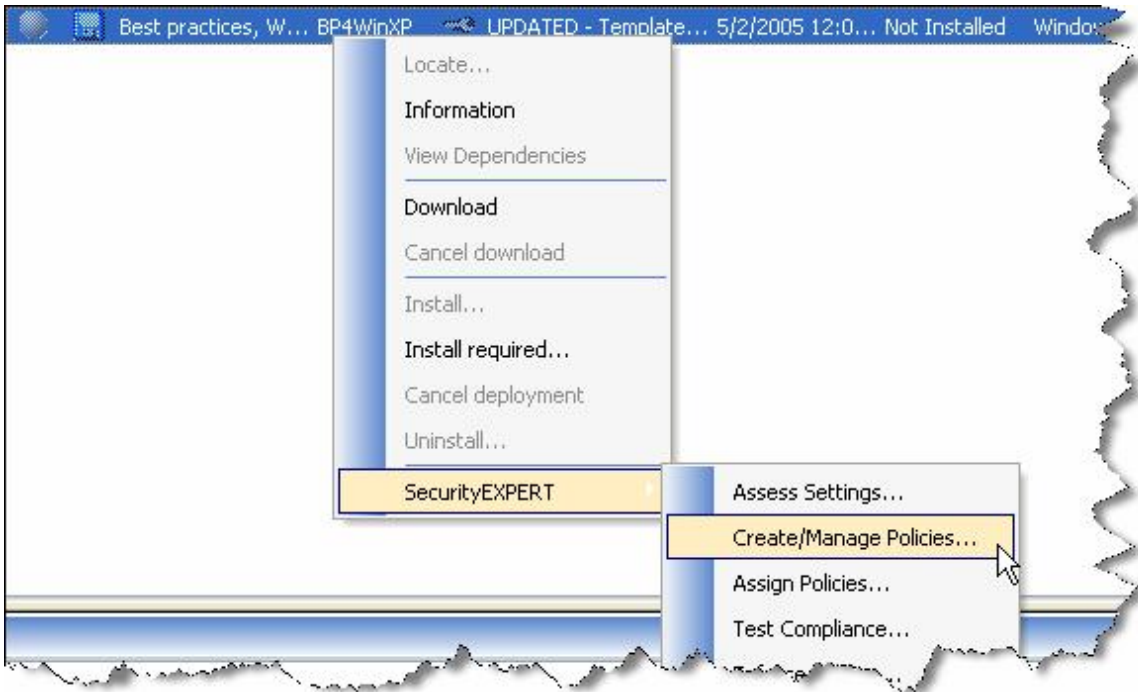
Once a named policy exists, the policy is assigned to one or more machines. Assessment and enforcement can then occur.

It is also possible to create a policy from scratch, focusing on specific items of interest. This may be appropriate for assessing and setting existing machines. This is what we will illustrate here.

Creating a SecurityEXPERT Policy

For purposes of this evaluation, let's create a very simple Windows XP policy so that assessment reports are easy to interpret. You may easily emulate this example for other platforms. You may create policies using two menu commands:

- **SecurityEXPERT > Policies ...**
- **Right-Click** on a Template (shown here) > **SecurityEXPERT > Create/Manage Policies**



Launch the Policy Manager as described above. *Downloaded templates* display in the "Manage Policies For:" pick-list. Select a template, and click **Create Policy** in the Policy Manager window.



SecurityEXPERT

Policy Setup

Policy Name: Date Created: 9/21/2005 Template: **Best Practices, Windows XP**

Author Name: Date Modified: 9/21/2005

Description:

(Optional)* Initialize new policy with values recommended by: Set Priority

<input type="checkbox"/> Select All	Expert	Website
<input type="checkbox"/>	NSA	www.nsa.gov/snac/
<input checked="" type="checkbox"/>	NIST	www.nist.gov
<input type="checkbox"/>	Microsoft	www.microsoft.com
<input type="checkbox"/>	CIS	www.cisecurity.org

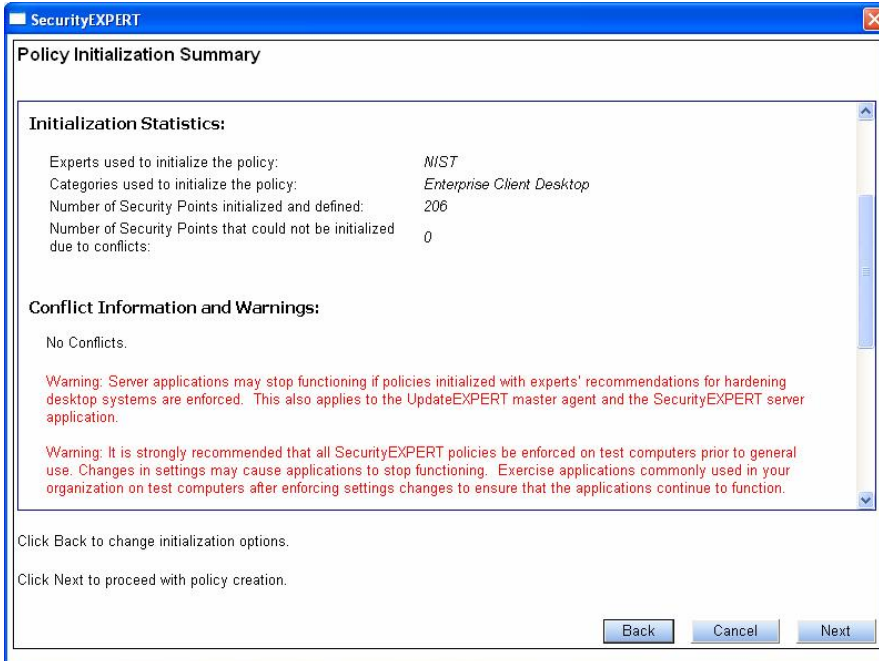
(Optional)* Only use values recommended for the following computer configurations:

<input type="checkbox"/> Select All	Category	Description
<input checked="" type="checkbox"/>	Enterprise Client Desktop	Enterprises are typically managed environments that are very structured in terms of hardware and software configurations.
<input type="checkbox"/>	Enterprise Client Laptop	Enterprises are typically managed environments that are very structured in terms of hardware and software configurations.

Include enforcement settings for Permissions and Auditing.

***Note: Initialization will only take place if at least one selection is made from both lists.**

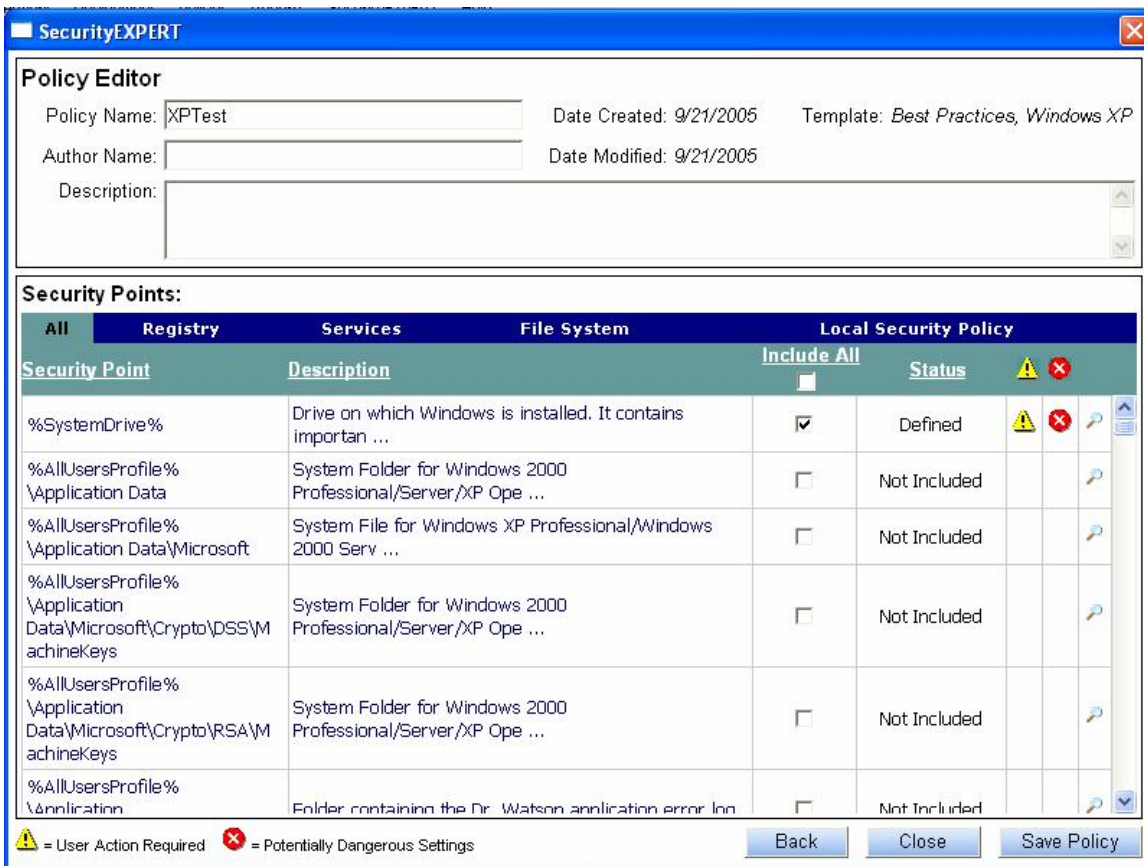
Enter a name for the policy (above). The selected template is highlighted on the right. To generate a list of security points to work with, check one or more experts, and check a machine configuration. This will determine the number of security points displayed. Click **Next**.



The policy initialization screen displays the chosen experts, configuration, resulting number of security points, and number of security point conflicts (one expert disagrees with another).

Also shown is general warning and expert disclaimer information.

Review this screen then click **Next**.



By default, ALL security points are listed under the All tab. Clicking **Registry**, **Services**, **File System**, or **Local Security Policy** groups related security points. Checked items on any tab are included in the policy based on the selected expert & machine configuration.

Policy Values: [Clear all values](#)

Settings:

Startup Type: Disabled

Status: Undefined

Enforcement Options:

Enforce Startup Type Enforce Permissions

Enforce Status Enforce Auditing

Permissions and Auditing:

Users/Groups: Everyone [Clear values](#)

[Add](#)

Permissions	Allow	Deny	Auditing	Success	Failure
	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

For our example, we want to assess **FTP** and **Telnet** services only. On the **ALL** tab, uncheck all defined items by checking "Include All", then unchecking "Include All." The result will be that all items are unchecked.

Note: An even easier way to start with no selected security points is to unselect all Experts and Categories on the "Policy Setup" screen. This allows start with 0 security points defined.

On **Services** tab, find FTP and click on the Magnifyer icon to pull up detail (← shown on left). Set the service to Disabled. Do not check the Enforce checkbox. Do the same for **Telnet**.

Rename the Policy to **XPServices** before Saving. **Note:** If you get a "Demo Mode" error when saving, contact support. You need your license enabled for settings.

Assigning the SecurityEXPERT Policy

XPServices will now be listed in the Policy Manager, but no computers have been assigned to the policy. Close the window. Select one or more applicable platforms, i.e., XP machines for an XP policy, right-click the template and select "**SecurityEXPERT > Assign Policies ...**"

SecurityEXPERT

Policy Assignment

Select a template to display associated policies: Best Practices, Windows XP

Available Policies:

	Policy Name	Description	Template Name
<input checked="" type="radio"/>	No Policies		
<input type="radio"/>	XPServices		Best Practices, Windows XP

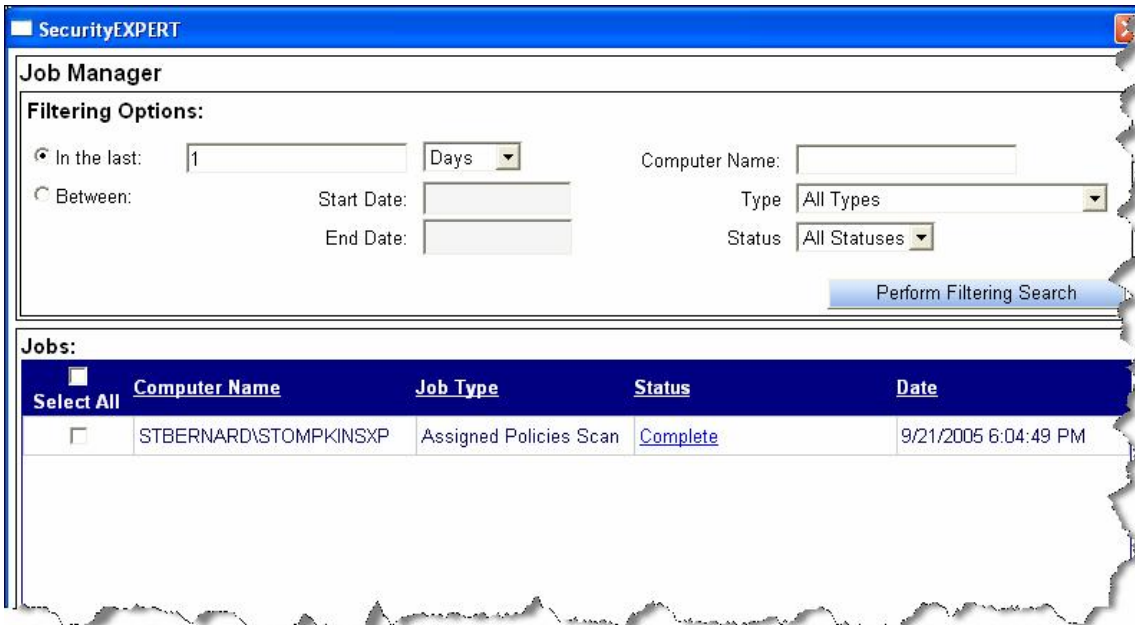
Select XPServices (see above) and click **Next**. Your selected machines are displayed. Click **Assign**.

Testing SecurityEXPERT Compliance

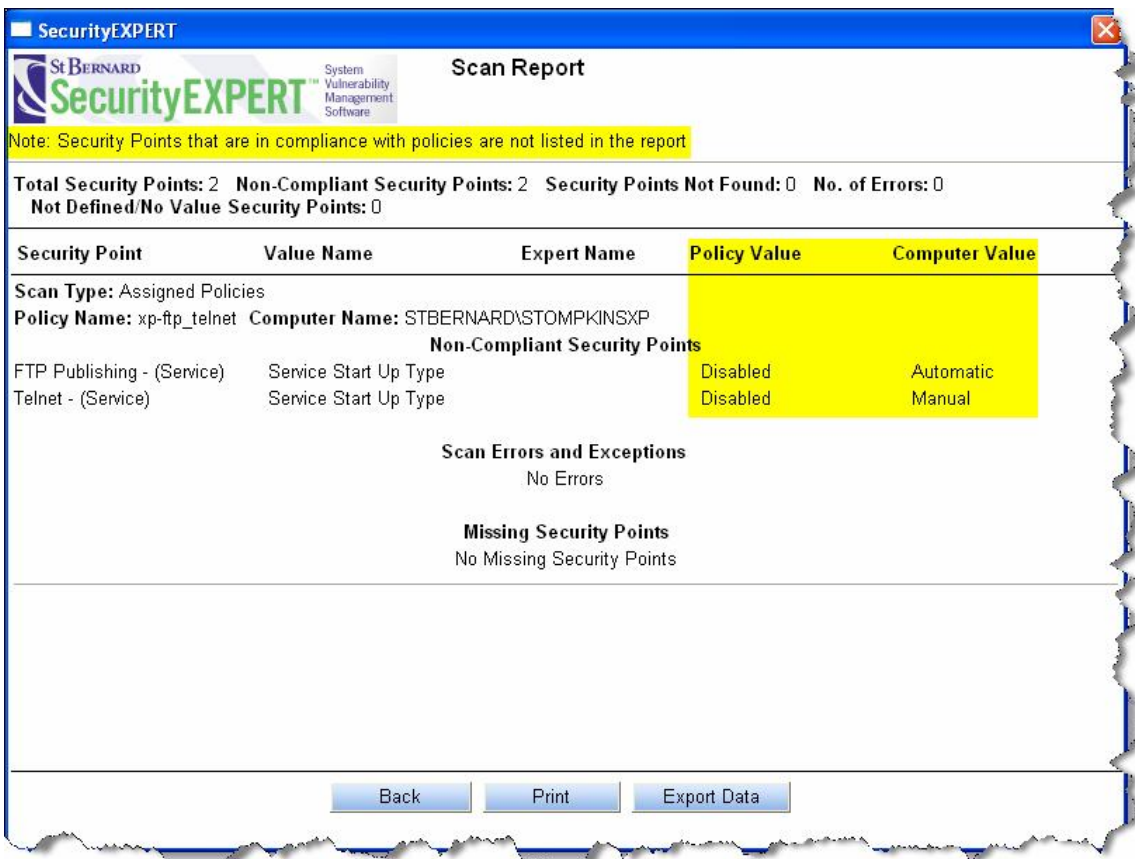
Assessing the status of the FTP and Telnet services on the target machines is a matter of testing compliance. Perform the following:

right-click the template and select "**SecurityEXPERT > Test Compliance ...**"

Note that the radio button defaults to "Assigned policies". Click **Next**, click **Scan Computers**, the Job Manager displays. Make sure **Auto-Refresh** is checked so you see the Status change



Clicking the **Complete** link (above) will display the assessment results (below).



Clearly FTP and Telnet are out of compliance. Note that nothing has been changed on the machines since we have not enforced the policy yet.

Modifying the SecurityEXPERT Policy

We now want to modify the policy for enforcement. Go to **SecurityEXPERT > Create/Manage Policies**, select your policy, and click **“View/Edit Policy.”**

Modify your security points, setting **Status:** to **“Stopped”** and checking the **Enforcement Options:** **“Enforce Startup Type”** and **“Enforce Status.”** See the screen shot below.

When enforcement is performed, the FTP and Telnet services will be stopped and disabled on the target machine. Because neither one of these services prevents remote access by UpdateEXPERT/SecurityEXPERT you will still be able to patch the machine and work with settings.

Note that you could have set enforcement options on the initial policy creation, avoiding this step. However, it is useful to modify an existing policy for learning purposes.

Also note that many expert recommended security points include enforcement options pre-selected. Recommended permissions for running a service or securing a file are often part of a security point, and are enforced when Enforce Permissions is checked.

Policy Values:

[Clear all values](#)

Settings:

Startup Type:

Status:

Enforcement Options:

Enforce Startup Type Enforce Permissions

Enforce Status Enforce Auditing

Permissions and Auditing:

Users/Groups: [Clear values](#)

[Add](#)

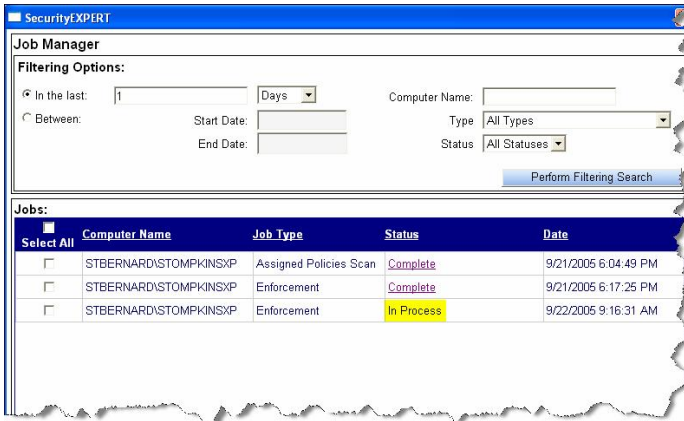
Permissions	<input type="checkbox"/>	Allow	<input type="checkbox"/>	Deny
Auditing	<input type="checkbox"/>	Success	<input type="checkbox"/>	Failure

Enforcing the SecurityEXPERT Policy

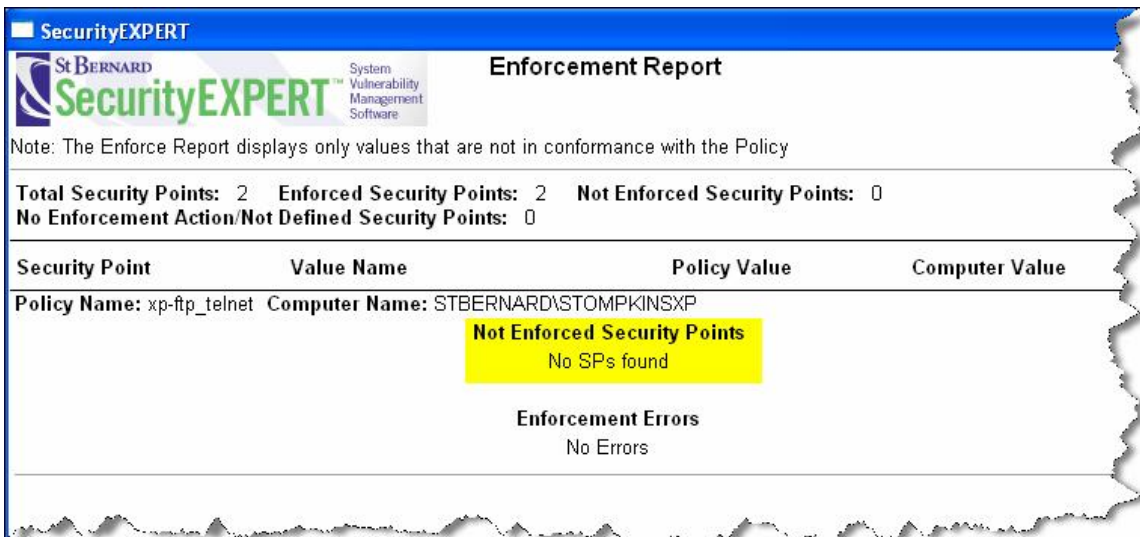
To enforce the policy, go to **“SecurityEXPERT > Enforce Policies ...”** and click **Enforce**. This will display the following dialogue box:



When you click **OK**, the settings will be applied. The **Job Manager** is launched and you will have an "In Process" job. Make sure **Auto-Refresh** is checked so you see the Status change.



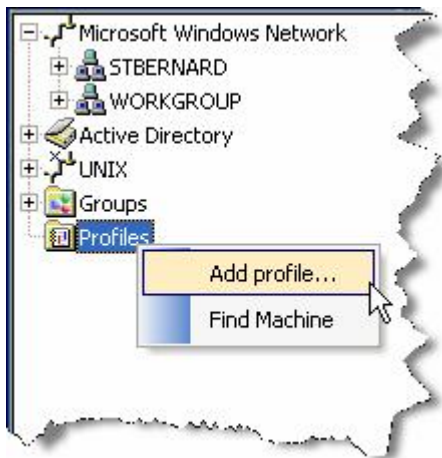
Clicking the **Complete** link will display the enforcement results (below).



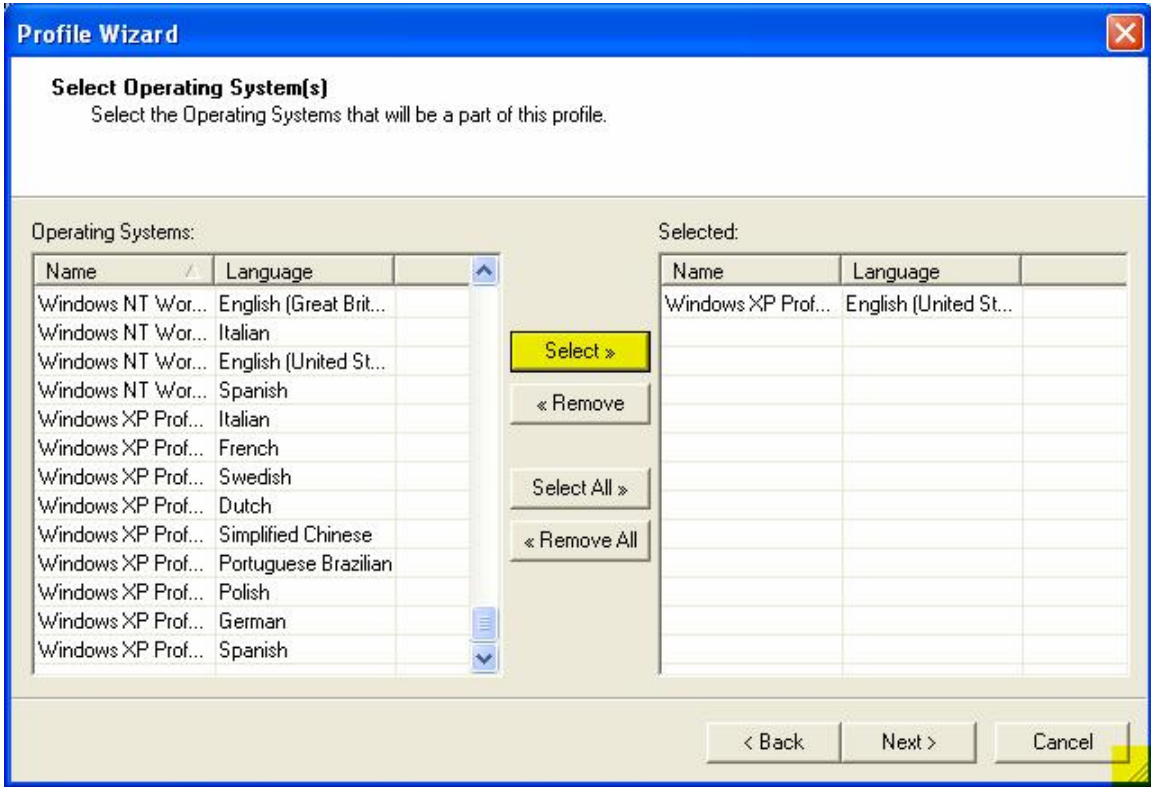
The machine is in compliance when no security points are listed.

Using Profiles with SecurityEXPERT

Templates are distributed per operating system platform. It may be helpful to create UpdateEXPERT profiles that group machines by Windows 2000 Professional, Windows 2000 Server, Windows XP Pro and Windows Server 2003 for policy assignment, assessment, and enforcement. Right-click the Profiles object in the network pane, and “**Add profile**” to launch the profile wizard.



Click **Next**, enter a profile name (XP for example), click **Next**, expand the profile wizard window (shown below) with a corner pull (highlighted below), find the OS to group, **Select** it (Windows XP English in this case), click **Next**, **Select** one or more Service-Pack levels, click **Next**, ignore the individual patches displayed, and click **Next** again (possibly twice) to complete your profile.



Your named object will show up under Profiles. Expanding the object will display managed machines that match the OS/Service-Pack(s) defined in your profile.

<p>The screenshot shows a tree view of 'Profiles' with 'XP' expanded. A context menu is open over the machines, with 'SecurityEXPERT' selected. The 'SecurityEXPERT' menu is also open, showing options like 'Test Full Compliance...' and 'Enforce All Policies...'.</p>	<p>Selecting machines, and right-clicking provides access to the SecurityEXPERT menu, where you can test compliance and perform enforcement.</p> <p>To assign a policy, right click on the template.</p> <p>To view which policies are assigned to which machines, use Create/Manage Policies, and click the Policy Assignment Manager button.</p>
---	---

This simple example gets you started with settings management. Please See **“Help > Contents”** in UpdateEXPERT Premium for more information on using SecurityEXPERT.

Glossary

- **Browser Pane:** The bottom pane within the Console that displays the UpdateEXPERT User Web page, detailed information about updates from Microsoft's web site, and results from the UpdateEXPERT reports.
- **Console:** The Console is the GUI front of UpdateEXPERT. The Consoles are used to view and manage the Master Agents
- **Enumeration:** The machine discovery process
- **Groups:** The Groups feature allows an administrator to manually create useful machine groupings. It can be found within the Network Pane.
- **Installer Service:** Replaces the NT Task Scheduler
- **Leaf-Agent:** Leaf-Agent is the term used for UpdateEXPERT's optional client-side software.
- **Managed Machines:** You need to use "Manage Selected" to identify the machines you intend to manage with UpdateEXPERT. This will decrement the licensed number of targets you can manage. Once a machine is "managed" it will be bold.
- **MLF:** Several machines can be added to the Network Pane by using "Machine List Files". After creating and saving a list of the IP addresses or names of machines, you can import it into the network view by selecting "Network | Import machine list..."
- **Network Pane:** The top left pane within the Console that displays machines within the network. This includes Microsoft Windows Network, Active Directory, Groups, and Profiles.
- **Profiles:** The Profiles feature will dynamically find machines according to specifications set by the administrator. The configurable specifications include operating systems, service pack levels, and installed patches. Profiles can be found within the Network Pane.
- **Named Policies:** The Policy menu supports the creation of multiple named policies that can be assigned to machines, and used for patch deployment and conformance reporting. This feature helps you define a **baseline** against which other machines can be measured.
- **Research View:** A list of every patch available in the UpdateEXPERT database.
- **Query:** Querying a machine will determine which patches are installed and not installed and uses that information to build a list that applies to each machine.
- **Settings:** Registry values, file permissions, services parameters, auditing, and local security policy items that can be set using SecurityEXPERT.
- **Smart Reboot Elimination (SRE):** "Smart Reboot Elimination" uses database information to determine what patches can be grouped to minimize reboots, what patches absolutely require a reboot, or whether a reboot is necessary at all. Having "Reboot" selected in the Patch Wizard installation options will take advantage of the S.R.E. feature.
- **Unified Master-Agents:** Multiple Master-Agents simultaneously connected to the Console for easier administration. The Master Agent is the administrative server component. It provides the research, inventory, deployment, policy, and validation of UpdateEXPERT.
- **UpdateEXPERT User Web Pane:** The browser pane's "home" page that contains links to the UpdateEXPERT knowledgebase and patch information database.
- **Updates Pane:** The top right pane within the Console that displays the patch lists for each machine, the Research View, and Custom Installs.
- **Validation:** Validation performs an inventory to confirm the integrity of installed patches on the target machines.

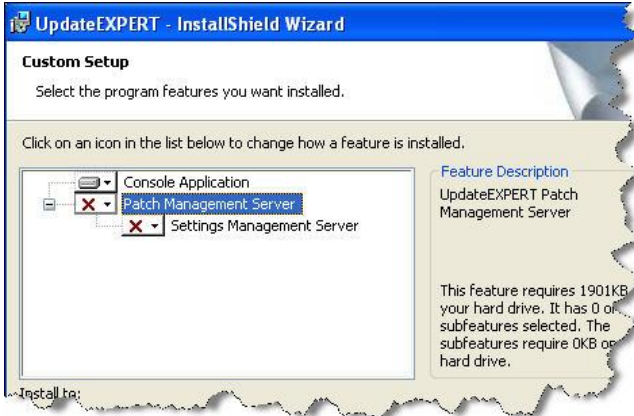
Thank You!

Thank you for taking the time to evaluate UpdateEXPERT Premium! Again, please do not hesitate to contact Technical Support if you wish to ask questions or get assistance.

Appendix A – Custom Install Options

Doing a “Custom” (instead of “Typical”) install allows you to specifically select which components you wish to install.

[Click here to return to Typical Install example.](#)



Install the Console Application and Agent-Installer components.

Useful for delegating patch management, or remotely connecting to one or more Master-Agents.

Note: The Agent-Installer is used for deploying Leaf-Agents and Master-Agents.



Exclude Settings Management Server (SecurityEXPERT) from the installation.

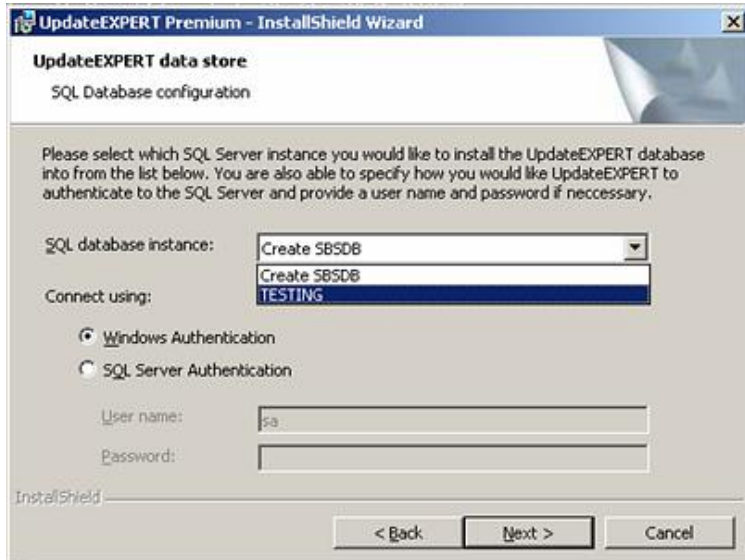


Install the Patch Management Server (Master-Agent and Agent-Installer).

Note: The Agent-Installer is used for deploying Leaf-Agents and Master-Agents.

Appendix A – Custom Install Options Continued...

“Custom” (instead of “Typical”) also allows you to specify an existing locally installed SQL instance for use, instead of MSDE. The UEDataStore and optionally SEDataStore databases will be created in MSSQL\$SBSDB folder for MSDE, or in MSSQL\$*LocalInstanceName* folder for SQL.



“Create SBSDB” means use MSDE. The result will be a folder called MSSQL\$SBSDB.

“Testing” is an existing Local SQL instance using a folder called MSSQL\$TESTING.

Note-1: Master-Agents are deployed with the Agent-Installer (File > Agent > Install Wizard...). The Agent-Installer also presents available Local SQL instances in a pick-list.

Note-2: Windows Authentication is always used for Patch Management. In v7.01, Settings Management also uses Windows Authentication by default, but allows using SQL Server Authentication as an option.